Altiris Client Management Suite 7.1 SP2 from Symantec User Guide for Mac Management

Symantec

Contents

Chapter 1 Introducing the Mac in Altiris Client Management Suite 7.1 from Symantec 9

About managing the Mac with CMS 7.1 9
Key CMS Mac capabilities and limitations compared to Windows 13
About supported package-delivery formats for software distribution 14

Chapter 2 Installing the agent and plug-ins for Mac 19

About installing the Symantec Management Agent for UNIX, Linux, or Mac 20
About the Mac Terminal and Secure Shell (SSH) 20
Symantec Management Agent for Mac installation prerequisites 21
Process for installing Symantec Management Agent for Mac 24
Setting up Notification Server name resolution with Mac computers 27
Disabling or configuring a built-in Mac OS X firewall 28
Allowing incoming connections through SSH 32
Installing Symantec Management Agent to the Mac OS X client computer 33
Checking the agent installation 34
About solution plug-ins for Mac 35
Command-line options for managing Mac client computers 35
About selecting Mac computers for a Symantec Management Agent manual installation 36
Selecting Mac computers for a Symantec Management Agent pull installation 37
Creating a .csv file for importing Mac computers 38
About installing the Symantec Management Agent for Mac with a push 39
Installing the Symantec Management Agent for Mac with a push 41
About installing the agent for Mac with a pull 42
Installing the Symantec Management Agent for Mac with a pull 43

Specifying the Symantec Management Agent for Mac installation settings 44
Installation Settings dialog box 45
Installation Settings: Connection and Authentication tab 46
Try connect by SSH using SSH Key authorization settings 47
Try connect by SSH using password authorization settings 48
Login and password settings 48
Timeout settings 50
Platform detection settings 51
Installation Settings: Agent Settings tab for Mac computers 51
Installation Settings: Install XML tab 52
About the Mac firewall and digitally signed packages 53

Chapter 3 Configuring the Symantec Management Agent for Mac 55

About configuring the Symantec Management Agent for Mac 55
Configuring the global agent settings 56
Symantec Management Agent Settings – Global: General tab 57
About the Tickle/Power Management settings 58
About the Package Multicast settings 60
Symantec Management Agent Settings – Global: Authentication tab 60
Symantec Management Agent Settings – Global: Events tab 60
Configuring the targeted agent settings on Mac computers 61
Targeted Agent Settings: General tab 64
Recommended Symantec Management Agent data update intervals 64
Targeted Agent Settings: UNIX/Linux/Mac tab 65
Targeted Agent Settings: Downloads tab 67
Targeted Agent Settings: Blockouts tab 70
Adding a blockout period to the targeted agent settings 71
Targeted Agent Settings: User Control tab 72
Targeted Agent Settings: Advanced tab 72
About maintenance windows for managed computers 73
Configuring maintenance window policies 74

Chapter 4 Discovering Mac computers on the network 77

About discovering Mac computers 77
Discovering Mac computers 77
Creating Network Discovery tasks using the wizard 79

Manually creating and modifying Network Discovery tasks 80

Chapter 5 Gathering inventory from Macs 83

About using Inventory Solution on Mac computers 84
About types of inventory tasks and data for Mac computers 85
Installing the Inventory Solution plug-in to the Mac OS X computer 86
About Inventory Solution for Mac 87
Gathering inventory information about Mac computers using a policy 88
Gathering inventory information using a task 90
About gathering custom inventory information about Mac computers 91
Gathering custom inventory information about Mac computers 92
About software inventory using the filescan.rule file on Mac computers 94
Using the filescan.rule file to run software inventory on Mac computers 96
Scanning for files on Mac computers using a custom file scan rule 96
Viewing inventory data of Mac computers in Resource Manager 97
Viewing inventory reports for Mac computers 97
Troubleshooting Mac problems with Inventory Solution 98
Enabling devnote logging on Mac computers 99
Ensuring that the Mac can receive the Inventory policy 99
Checking deployment of the Inventory Solution plug-in to the Mac OS X computer 100
Checking the inventory information that is gathered with a policy 101
Checking the inventory information that is gathered with a task 102
Installing the Inventory Solution plug-in on Mac client computers 102

Chapter 6 Software Management Solution for Mac 105

About delivering Mac software with Software Management Solution 106
Components of Software Management Solution specific to Mac computers 107
What you can do with Software Management Solution on Mac computers 108

Implementing Software Management Solution on Mac computers 109
About the agents and plug-ins that Software Management Solution uses 110
About Software Management Solution settings for Mac computers 111
Schedule settings for Managed Software Delivery to Mac computers 112
Download settings in Software Management Solution for Mac computers 114
Run settings in Software Management Solution for Mac computers 115
Results-based actions settings in Software Management Solution for Mac computers 116
Advanced options in Managed Software Delivery policies for Mac computers 117
Advanced options for tasks in Software Management Solution for Mac computers 118
Methods for delivering software to Mac computers 119

Chapter 7 Managed Software Delivery to Mac computers 121

About advanced software deliveries 121
Advanced delivery actions that Managed Software Delivery can perform with Mac computers 122
About the execution of Managed Software Delivery policies on Mac computers 123
About software policy remediation on Mac computers 126
Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers 127
Select Software dialog box 128
Policy Rules/Actions section for Mac computers 129
Policy Rules/Actions: Software tab for Mac computers 129
Policy Rules/Actions: Policy settings tab for Mac computers 131
About the Software Portal 132

Chapter 8 Using scripts to deliver tasks to Mac computers 133

About using tasks to manage Mac computers 133
About configuring a software delivery task for Mac computers 134
Configuring a software delivery task 134
Creating a DMG file to deliver software to Mac OS X computers 136

Creating an Installer Shell script to deliver software to Mac OS X computers 137
Importing an installer into the Software Catalog to deliver software to Mac OS X computers 138
Creating a task to disable the Product Improvement pop-up 140
Creating a Managed Software Delivery policy to deliver software to Mac OS X computers 140

Chapter 9 About Mac Patch Management 143

About patching Mac software 143
About how Mac patching works 144
About hosting an internal SUS to obtain internal software updates 144
Redirecting a Mac client computer to a local SUS 145

Chapter 10 Patch Management Solution for Mac 149

About Patch Management Solution for Mac 149
Implementing Patch Management Solution for Mac 150
Checking for available software updates 151
Viewing the list of available software updates 152
About installing software updates 152
Installing individual software updates 152
Installing all updates 154
Patch management for Mac return codes 155
About Patch Management Solution for Mac reports 155
Viewing reports 156
About the Mac compliance dashboard 157

Chapter 11 Remote control with Mac computers 159

About remote control with the Mac 159
pcAnywhere communication requirements 161
pcAnywhere Connection tab 161
pcAnywhere Authentication tab 162
pcAnywhere Access Server tab 162
Installing the pcAnywhere plug-in 163

Appendix A Mac imaging 167

About setting up the Mac imaging environment 168
System requirements for Mac imaging in Deployment Solution 6.9 169
About the limitations of imaging Mac computers 171

About using Deployment Solution 6.9 to manage and image Mac computers 172
Using Deployment Solution 6.9 to manage Mac computers 172
Using Deployment Solution 6.9 to image Mac computers 174
Performing management tasks 176
About Installing Mac OS X Server software 177
Creating a Mac OS X automation image 178
Installing Mac OS X 182
Customizing the source OS 183
Installing the Darwin ADLagent 184
Enabling Darwin ADLagent logging 185
Converting the Darwin ADLagent to an automation role 186
Adding Share credentials to the source keychain 187
Capturing the source image 187
Creating the NetBoot image using the System Image Utility 189
Setting up the NetBoot service 189
Performing imaging tasks 190

Appendix B Troubleshooting 193

About Symantec Notification Manager 193
Installing the Symantec Management Agent for Mac 193
Launching the Symantec Management Agent for Mac GUI 194
Using the Symantec Management Agent for Mac GUI 194

Index 199

Chapter 1

Introducing the Mac in Altiris Client Management Suite 7.1 from Symantec

This chapter includes the following topics:

- About managing the Mac with CMS 7.1

About managing the Mac with CMS 7.1

You can manage Mac computers with Altiris Client Management Suite (CMS) 7.1 from Symantec in much the same way that you manage Windows computers. However, some of the differences that exist are significant.

This topic and related topics present the information that you need to discover and manage the Mac computers that are already in your network.

Before you begin to discover and manage Mac computers, Symantec recommends that you do the following:

- Define your goals with regard to Mac computers.
  Consider the number of departments among which the Mac computers are distributed. Assuming that Mac computers are in the minority on your network, they may be spread among departments as diverse as engineering and business operations.
  Determine whether you need to image and manage Mac computers or if you only need to manage them.
- Determine the extent to which you need to manage Mac computers.
  If you want to know where the Mac computers are, you may only want to use discovery policies. Perhaps you want to deliver software, patch the Mac

computers with software updates, or manage Mac computers remotely. When you have a good idea about what you want to manage, consider how the policies that you roll out may affect all Mac computers. In other words, a policy that applies to Mac computers in an engineering department may not be useful for Mac computers in other parts of the company.

- Based on your planning, select the discovery tasks and management tasks to perform.
  You may already have policies in place to accomplish those goals. If you want to accomplish different goals with Mac computers than with Windows computers, then you may need to create Mac-specific policies. You may determine that you need to create one policy to accomplish your discovery goals or management goals for all Mac computers. Or, you may need to create a unique policy for Mac computers in each department.

Because you are already familiar with managing Windows computers in CMS, the learning curve for managing Mac computers is not burdensome. Symantec designed CMS to mirror processes for Windows and Mac computers to the extent possible, considering the inherent differences in the two platforms. An example is software packages. For Mac, you might import a DMG software package. This software package works the same way for Mac computers as a compressed or .zip file works for Windows computers. Note, however, that not all Mac packages "translate" easily to a Windows environment.

See "About supported package-delivery formats for software distribution" on page 14.

Common network functions such as file import and software delivery work in much the same way for Mac computers as they do for Windows. You already know much of what you need to know because of working with Windows computers and CMS.

Installing the agent for Mac computers on the network is like installing them for Windows computers. After you install Symantec Management Agent for Mac, you turn on the solution plug-ins. The solutions that you have installed use policies to install their solution plug-ins. In some cases you must install a plug-in. These cases are documented in the chapters in which those plug-ins are used.

See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 20.

Network Discovery works in much the same way on all platforms. However, on Mac computers you must enable SNMP if you want Network Discovery to display a discovered Mac as a computer resource. If you do not enable SNMP, Network Discovery displays each Mac computer as a generic network device such as a router, switch, or hub. You can enable SNMP on each Mac, or you can enable File and Printer Sharing.

See "About discovering Mac computers" on page 77.

Symantec Management Platform offers a built-in inventory function that is known as *basic inventory*. Basic inventory consists of the data that you can gather when the Symantec Management Agent is installed on the managed client computer. This inventory is a core function of Symantec Management Platform and does not require Inventory Solution Plug-in to be installed. Basic inventory gathers information such as computer name, domain, installed operating system, MAC and IP address, and primary user account. This information is updated on a regular basis as long as the Symantec Management Agent is installed on the computer.

Inventory Solution lets you gather additional inventory information. When you install Inventory Solution and turn on the Inventory Solution plug-in, you can gather additional inventory information on network computers, including Mac computers. Gathering inventory information about Mac computers on the network is similar to gathering inventory information about Windows computers. The agent on the Mac reports in on the same schedule, and you gather inventory information in Symantec Management Console. In the console you select advanced software inventory settings and click the **Run Options** tab. Under that tab you see the **Access network file systems (Mac/Linux/UNIX)** option and under **Software Scan Settings** for **Drives**, **Folders,** and **Files** you can then see Mac options. The difference between Windows inventory and Mac inventory is that with Mac, you must specify the options.

See "About using Inventory Solution on Mac computers" on page 84.

Inventory Solution also lets you gather custom inventory from Mac computers. You can gather hardware and software information beyond typical inventory tasks. One example is that you may want to locate a CD key for a certain product. Or, you may want to locate some other information that is specific to a computer. You create a custom inventory to gather information about anything on your network by writing your own script to identify the information to gather.

See "About gathering custom inventory information about Mac computers" on page 91.

Managing software is quite straightforward for Mac computers, although it is a little different from the Windows process. Differences include unique Mac terminology; for example, you *update* Mac software whereas you *patch* Windows software. Another difference is that with Windows computers you download software to Notification Server and push it to managed computers. With Mac computers you create a task to initiate the software update utility that is built in to Mac computers. You also deliver patches (software updates) to Mac computers using tasks and jobs rather than policies. A great deal of the Software Management Solution documentation applies equally to Mac computers and Windows computers. The following cross-reference links to Mac-specific information about software management.

See "About delivering Mac software with Software Management Solution" on page 106.

The Symantec Software Portal is users' self-service software resource. For Mac computers, the Software Portal works very much like it does for Windows computers. The Software Portal is useful if you want to let end users install software by requesting or downloading the software that they need. The Software Portal does not rely on proprietary controls such as ActiveX. This lack of reliance on proprietary controls means that users on any platform can access the software that you configure as applications in the portal.

See "About the Software Portal" on page 132.

An important difference between managing software on Mac and Windows computers is that on Mac computers the software detection process and the compliance process are manual. On Mac computers, you can set up dependencies and then run tasks to manage software. You can use inventory tasks to find out which applications are installed. Then you can execute a command-line script or use another manual process to delete the applications that are not allowed. This process is different from software detection with Windows computers, where unallowed applications are deleted automatically.

To patch Mac software, you run an update task to see if the Mac computer needs updates. The agent checks the Mac software and reports results. In Symantec Management Console you view the results in a report. In the console, you can click each instance of out-of-date software and then create a policy to install the updates. CMS contacts the Mac OS X client computer and prompts the Mac to run its own built-in software update utility. This utility causes the Mac to install all available software updates. In this way the Mac keeps its OS and software up to date, which is more comprehensive capability than Windows computers have. The update engine produces a report that is displayed in Symantec Management Console.

See "About patching Mac software" on page 143.

A common way to deliver tasks to Mac computers is by creating and running scripts. Because this method may be new to you, the task chapter includes general information and a sample software-delivery task.

See "About using tasks to manage Mac computers" on page 133.

A subset of the pcAnywhere Solution remote-control functions is also available with Mac computers.

See "About remote control with the Mac" on page 159.

If you plan to image Mac computers, be aware that process of imaging a Mac is substantially different from the process of imaging a Windows computer. Significantly, not all features of Deployment Solution apply to Mac OS X computers. Imaging for Mac computers is part of Deployment Solution 6.9 SP3, SP4, and SP5.

Your Deployment Solution 7.1 solution includes the license for DS 6.9; however, you must install it before you can use it to create Mac images. Common reasons for imaging a Mac include a virus that ruins one or more managed Mac computers. You may want to re-use a Mac, and in this case you can re-purpose it by using an image that suits your needs. You may want to upgrade a Mac OS, which you can do from the managed Mac over the network.

Mac imaging uses the NetBoot service rather than PXE and WinPE. Whereas on a Windows computer you use WinPE to boot into a preboot environment, on a Mac you use NetBoot. You use the NetBoot service on Mac OS X Server to create the preboot environment. Although you can use other methods to image Mac computers, Symantec supports only the method that is presented in this guide.

See "About setting up the Mac imaging environment" on page 168.

Refer to the following resources for general information about Mac computers:

- Apple Mac OS X Server user guides for beginning and advanced users
- Apple Mac OS X Server overview
- The Apple knowledge base (requires a login)
- *Macworld* article Mac support in an Active Directory environment
- Mac management community on Symantec Connect (requires a login)

Key CMS Mac capabilities and limitations compared to Windows

Altiris Client Management Suite (CMS) 7.1 from Symantec was designed with Windows and Mac computers in mind.

See "About managing the Mac with CMS 7.1" on page 9.

Most Windows capabilities are also offered for Mac computers. One example is that you discover and manage Mac computers in much the same way that you discover and manage Windows computers. Noticeable limitations are listed because they are to be resolved in a future release.

In the table, Yes in the Mac or Windows column indicates that the capability exists for that platform. Some Mac capabilities are not applicable to the Windows platform, and this condition is marked in the table as N/A.

Table 1-1 Comparison of key CMS Mac capabilities and limitations with Windows

CMS capability	Mac OS X	Windows
Network Discovery	Yes	Yes

Table 1-1 Comparison of key CMS Mac capabilities and limitations with Windows *(continued)*

CMS capability	Mac OS X	Windows
NetBoot Imaging	Yes	N/A
Hardware, software, and user inventory	Yes	Yes
Software delivery	Yes	Yes
Platform-specific agent UI	Yes	Yes
Agent UI is localized	Future release	Yes
Intelligent software management	Yes	Yes
Software detection rules See "About delivering Mac software with Software Management Solution" on page 106.	Future release	Yes
Application metering	Future release	Yes
Self-service Software Portal (IE, Firefox, and Safari)	Yes	Yes
Remote control (pcAnywhere)	Yes	Yes
Automated software updates (Patch Management Solution)	Yes	Yes
Advanced software inventory	Yes	Yes
Custom inventory	Yes	Yes
Cross-platform reporting	Yes	Yes
Power control (Wake Up, Log Off, Restart, Shut Down)	Yes	Yes
Snow Leopard (10.6) support	Yes	N/A
Native DMG file support	Yes	N/A

You should also be aware that Deployment-Solution-equivalent functions such as copy file are not yet offered for managing Mac computers in CMS.

About supported package-delivery formats for software distribution

Apple extensions for software packaging and distribution can complicate some Symantec Management Platform tasks that are carried out by Notification Server.

See "About managing the Mac with CMS 7.1" on page 9.

The Apple Mac OS X GUI presentation of DMG, PKG, MPKG, and APP extensions can introduce confusion for you and other Windows administrators. Confusion can arise particularly when you need to manage Mac OS X software from Notification Server: Perform transfer tasks, software import tasks, and software delivery tasks with a software push initiated from an OS other than Mac OS X.

However, Notification Server has built-in functionality to import software for Mac OS X in its repository. From that repository you can schedule distribution of the software through Quick Delivery, a Managed Software Delivery policy, or an offline task.

This topic describes the packaged software presentation under Mac OS X. It explains how DMG, PKG, MPKG, and APP files and directory extensions do and do not relate to Windows file formats and extensions. This information helps you understand how Symantec solutions and the agent platform support Apple software distribution.

Software Management Solution in Altiris Client Management Suite 7.1 from Symantec supports the following delivery media for Mac computers:

- Apple Disk Image: DMG
  A DMG is an archive similar to a Windows ISO
- Installation packages: PKG and MPKG
  These installation packages are most closely related to Windows MSI files.
- Application bundles: APP
  Mac application bundles have no Windows equivalent.

Windows file formats	Related Mac file formats

ISO

DMG

Mac OS X files with ".dmg" extension are Mac OS X disk image files (DMGs). A DMG is a Mac OS X proprietary format CD/DVD ROM image. A DMG is similar to an ISO file and to Apple CDR files. It represents an upgrade to Mac legacy IMG files.

To store Mac software on the Windows NTFS file system, Symantec requires that you first compress the software application files into an Apple DMG. You can create a DMG using utilities that are bundled with Mac OS X. One such example is Disk Utility.

After the application is compressed into a DMG, you mount the DMG on a Mac in the same way you mount a CD-ROM drive.

The key DMG characteristics or features that are not available in ISO are as follows:

- Are in over-the-Internet distribution form for Mac OS X software.
- Behave like disk volumes.
- Can be mounted to a mount point on Mac OS X.
- May contain multiple partitions with Apple's proprietary HFS+ filesystem.
- Are convertible to ISO images using Mac OS X Disk Utility.

The key DMG characteristics or features that set it apart from ISO are as follows:

- Preserves the extended attributes of the packaged software.
- Allows secure password protection.
- Allows encryption.
- Allows compression.
- Can be an image of an optical disc.
  The actual HDD ISO 9660 is primarily used for optical disc imaging.
- Apple-proprietary format specific to Mac OS X.
  ISO 9660 is a cross-platform non-proprietary standard.

DMG files are regular files and are presented that way in Finder.

The power of DMG files is that they can be transferred between various operating systems, preserving all the attributes of the enclosed application or data.

MSI	PKG
	A PKG is an Apple installation package. This package can be a file package with the .pkg extension or a file package with the .mpkg extension. Installation packages contain products or product components. The products or components are known as the package payload. The installation package also contains the installation information that the Installer application and the Remote Desktop use to place product files on a file system. A PKG can be a file or a folder.
MSI	MPKG
	An MPKG is an Apple metapackage. A metapackage is an installation package that contains other installation packages. These other installation packages are usually component packages. A metapackage delivers the products that include multiple components. The metapackage gives users the installation options that let them select the components to install. You can combine multiple packages into a metapackage. Before you transfer one or more metapackages to another Mac, Windows, or other computer, you must roll it into an archive. You must roll metapackages into an archive to preserve the directory structure, permissions, and other attributes during the transfer. Archives include TAR, ZIP, TAR.GZ, or TAR.Z. An MPKG can be a file or a folder.
	APP
	Application bundles do not have a Windows equivalent.

Chapter 2

Installing the agent and plug-ins for Mac

This chapter includes the following topics:

- About installing the Symantec Management Agent for UNIX, Linux, or Mac
- About the Mac Terminal and Secure Shell (SSH)
- Symantec Management Agent for Mac installation prerequisites
- Process for installing Symantec Management Agent for Mac
- About solution plug-ins for Mac
- Command-line options for managing Mac client computers
- About selecting Mac computers for a Symantec Management Agent manual installation
- Selecting Mac computers for a Symantec Management Agent pull installation
- Creating a .csv file for importing Mac computers
- About installing the Symantec Management Agent for Mac with a push
- Installing the Symantec Management Agent for Mac with a push
- About installing the agent for Mac with a pull
- Installing the Symantec Management Agent for Mac with a pull
- Specifying the Symantec Management Agent for Mac installation settings
- Installation Settings dialog box
- Installation Settings: Connection and Authentication tab

- Installation Settings: Agent Settings tab for Mac computers
- Installation Settings: Install XML tab
- About the Mac firewall and digitally signed packages

About installing the Symantec Management Agent for UNIX, Linux, or Mac

In the context of managing Mac computers in CMS, installation refers to installing the Symantec Management Agent for UNIX, Linux, or Mac. This ULM agent is a unified agent that runs on the UNIX-based operating systems. In the Symantec Management Console, this agent is labeled **Symantec Management Agent for UNIX, Linux, or Mac**. In documentation referring to managing Mac computers, it is commonly referred to as Symantec Management Agent for Mac or as Symantec Management Agent.

See "About managing the Mac with CMS 7.1" on page 9.

In Symantec Management Console, Symantec Management Agent for UNIX, Linux, or Mac is one of your installation options.

Installing Symantec Management Agent for UNIX, Linux, or Mac is different in some ways from installing the Windows agent. Refer to the installation prerequisites and the installation process table for details.

See "Symantec Management Agent for Mac installation prerequisites" on page 21.

See "Process for installing Symantec Management Agent for Mac" on page 24.

About the Mac Terminal and Secure Shell (SSH)

You can run terminal commands at the Mac Terminal, which is on the physical client computer. Using the terminal app on a Mac client computer is equivalent to opening a DOS prompt on a Windows client computer. If you do not have access to the physical computer, you can perform "Terminal" commands on a client computer through an SSH session.

The path to the terminal application on a Mac computer is **Finder > Applications > Utilities > Terminal App**.

Refer to the following Apple documentation:

- Mac OS X 10.6 Help Allowing a remote terminal to access your computer for additional information about remote terminal access using SSH
  You can easily find the same topic for other versions of OS X.

- Mac OS X Server Command-Line Administrationfor additional information about the terminal app and SSH.

See "Allowing incoming connections through SSH" on page 32.

See "Symantec Management Agent for Mac installation prerequisites" on page 21.

Symantec Management Agent for Mac installation prerequisites

Mac software runs only on the hardware that is designed to support it. In this way, system requirements for managing Mac computers are simpler than Windows.

Your computer must meet the hardware prerequisites and software prerequisites before you can install the Symantec Management Agent.

See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 20.

Table 2-1 Symantec Management Agent for Mac installation prerequisites

Prerequisite	Description
Operating system	Any of the following operating systems: ■ Mac OS X 10.4.x (Universal binary), 10.5.x (Universal binary), 10.6.x (Universal binary) ■ Mac OS X Server 10.4.x (Universal binary), 10.5.x (Universal binary), 10.6.x (Universal binary) Universal binary means that the OS 10.x can run on either a PowerPC or an Intel computer.
Hard disk space	35-MB minimum for temporary installation files and 35 MB for resident installed files
RAM	15-MB minimum
Microsoft IIS	Before you configure any computers as site servers or package servers, you must install IIS on those computers. You must install and properly configure IIS on all site servers and package servers to create HTTP codebase entries and download packages. All Mac agent communication is done through HTTP. Without IIS, the HTTP codebase entries are not created and distributed to Mac client computers. If the entries are not created and distributed, you cannot download packages. This failure also prevents you from downloading the solution plug-in installation packages.

Table 2-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Access rights	Symantec requires administrator account credentials to connect to ha client Mac computer. After you connect to the Mac as a local administrator, you can either push or pull the agent. You push the agent automatically from Symantec Management Console or pull the agent manually, from the Mac Terminal. In CMS 7.1 and earlier, explicit root privileges were required for installing the agent. If you have upgraded to CM 7.1 SP1 or later you gain root privileges in the background when you do a push installation using the administrator account credentials. If you do a pull installation, you connect to the Mac computer as an administrator and at the Mac Terminal run the `sudo ./aex-bootstrap-macosx` command. The sudo command gives you root privileges on the Mac computer and you can install the Symantec Management Agent. When you perform a remote installation of the agent from Symantec Management Console, you install the agent using a local administrator account. This account is required for all installation methods, including push and pull. The concept of a root directory and root user may be new if you have worked only on the Windows platform. The root user is not synonymous with the Windows administrator account. Root is a particular user on UNIX-style operating systems. It is a powerful account, and you should understand it thoroughly before you enable, disable, or use it. You can find an introduction to the concept of the root user at the Apple support site in Enabling and using the "root" user in Mac OS X and in HOWTO2518 in the Symantec Knowledge Base. If you have difficulty using the Apple link, use this URL: http://support.apple.com/kb/HT1528?viewlocale=en_US. **Note:** The remote installation page in Symantec Management Console by default suggests that you use the root account to install the Symantec Management Agent for Mac. This account is required only if you plan to install the pcAnywhere plug-in at some point. If you plan to install the pcAnywhere plug-in, then you must specify `root` in the **Privileged account login** field. Enter the password for the root account in the **Privileged account password** field. These actions let you install the pcAnywhere plug-in successfully.

Table 2-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Remote SSH connections enabled, if required	Only a push installation from Symantec Management Console requires that you enable remote login through Secure Shell (SSH) on the destination Mac client computer. You enable SSH in **System Preferences** in the **Sharing** window. To enable SSH, enable **Remote Login**. The Secure Shell (SSH) gives you access from Symantec Management Console (specifically, Notification Server) to remote Mac client computers. Without SSH enabled, you cannot install the agent. With SSH enabled, you can perform bulk installations of the agent from Notification Server to multiple Mac clients. **Warning:** Load the same type of shell that you specify in the environment; for example, if you load a Bourne shell, specify a Bourne shell. Do not load a Bourne shell and then specify a C shell. The shell that you use must match the type that you specify. To allow an incoming SSH connection, ensure that an SSH server is running on the Mac client computer and that the firewall is configured. See "Process for installing Symantec Management Agent for Mac" on page 24. See "Allowing incoming connections through SSH" on page 32. **Note:** If you install through a manual process or a pull installation, you do not need to enable SSH. For a pull installation, you download `aex-bootstrap-macosx`. This self-extracting script triggers the agent installation. To use this script, you use the `sudo` prefix from the Mac Terminal. The Mac Terminal is synonymous with the Windows command line. See "Command-line options for managing Mac client computers" on page 35.
Outbound connection to Notification Server is enabled	You must configure the firewall to allow an outgoing connection to a Web port on Notification Server. See "Process for installing Symantec Management Agent for Mac" on page 24. See "Disabling or configuring a built-in Mac OS X firewall" on page 28. Notification Server communicates through port 80 by default through an outbound connection. The agent communicates through Notification Server through port 80 (HTTP, for browsing) or port 443 (HTTPs, secure). The agent communicates with Notification Server over HTTP or HTTPs; therefore, you must configure the firewall to allow whichever type of connection you choose to allow.

Table 2-1 Symantec Management Agent for Mac installation prerequisites *(continued)*

Prerequisite	Description
Notification Server name resolution is set up	Set up Notification Server name resolution. See "Process for installing Symantec Management Agent for Mac" on page 24. You can set up name resolution in one of the following ways: ■ Set up name resolution through DNS. ■ Add the host name and IP address of Notification Server to the `/etc/hosts` file on the Mac client computer. See "Setting up Notification Server name resolution with Mac computers" on page 27. See "Command-line options for managing Mac client computers" on page 35. Symantec does not recommend using the option to use only the Notification Server computer IP address. This option requires reconfiguration of the Notification Server computer codebase and snapshot settings. For details, see HOWTO3674 in the Symantec Knowledge Base.
Push-installation requirements are met	If you plan to install the agent through a push, you must remove or disable the customized prompts and the login scripts that include interactive prompts. Customized prompts can cause a push installation to fail. Customized prompts are those that are multi-lined, contain colors, contain more than 200 characters, or have been customized in any other way. Login scripts that users run cannot include interactive prompts, because the Symantec installation scripts cannot detect or respond to those interactive login scripts on Mac client computers. You do not need to discover Mac computers on your network with Network Discovery before you push the agent to those computers. See "About installing the Symantec Management Agent for Mac with a push" on page 39.

Process for installing Symantec Management Agent for Mac

Installing the agent for Mac is a process that includes several primary tasks. Click the link in the **Notes** column to learn more or follow procedures. Then, click the link back to this process table to ensure that you successfully complete each installation step.

See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 20.

You install the agent on client computers in one of the following ways:

- Automatically
  Push the agent from Symantec Management Console to the client Mac computer. This method is the best practice. It is the most common method and is described in the following table.
- Manually
  The options are explained in the following table.

Table 2-2 Process for installing the agent for Mac

Step	Description	Notes
Step 1	Prepare for installation.	On the Symantec Management Platform computer and on the Mac client computer or computers, close unnecessary applications.
Step 2	Select the Mac computers to which you want to install the agent and plug-in. You have the following options for selecting computers: ■ Network Discovery ■ Manual selection by adding client host names or IP addresses ■ Active Directory Import ■ Import using a comma-separated values file..	See "About selecting Mac computers for a Symantec Management Agent manual installation" on page 36.

Table 2-2 Process for installing the agent for Mac *(continued)*

Step	Description	Notes
Step 3	Prepare the Mac client computer or computers for agent installation. Ensure that you have met the prerequisites, as follows: **1** You have the correct access to Mac computers. **2** You have enabled a Secure Shell (SSH) for push installations. Pull installations do not require SSH. You connect to the Mac client computer through SSH and log in to the client using administrator credentials. You must specify the administrator credentials in **Installation Preferences** on the managed Mac. **3** You have resolved the Notification Server computer name. **4** The Mac firewall is disabled.	For explanation or details, refer to the prerequisites. See "Symantec Management Agent for Mac installation prerequisites" on page 21. Each Mac client computer may have a different administrator user. You must log in to each computer using the administrator credentials for that client or you get a login error. If you need help with the shell, Apple Server Admin 10.6 Help may be useful to you. You can enter the following URL without spaces if you have difficulty using the link: http://docs.info.apple.com / article.html?path=ServerAdmin / 10.6/en/xg6d3f7fe1.html. See "Allowing incoming connections through SSH" on page 32. The managed Mac must be able to resolve the Notification Server computer by name, not by IP address. The fully qualified domain name may be required. See "Setting up Notification Server name resolution with Mac computers" on page 27. See "Disabling or configuring a built-in Mac OS X firewall" on page 28.
Step 4	In Symantec Management Console, specify agent configuration settings	See "Specifying the Symantec Management Agent for Mac installation settings" on page 44.

Table 2-2 Process for installing the agent for Mac *(continued)*

Step	Description	Notes
Step 5	Deploy the Mac agent. An automated installation is done from Symantec Management Console and is known as a push installation. A manual installation is done from the Mac client computer and is either a pull installation or a command-line installation. Note that you do not typically install plug-ins on the Mac. Each solution has its own plug-in. In most solutions, solution policies install these solution plug-ins after the Mac agent is installed. However, you may need to enable the plug-in policies. Refer to solution-specific documentation to find out how each solution plug-in works. See "About solution plug-ins for Mac" on page 35.	You can install the agent by a push or a pull, as follows: ■ Push from the console. A console push is the most common Mac agent installation method and is the best practice. See "About installing the Symantec Management Agent for Mac with a push" on page 39. See "Installing Symantec Management Agent to the Mac OS X client computer" on page 33. ■ Pull the agent from Symantec Management Console to the client Mac computer. See "About installing the agent for Mac with a pull" on page 42. ■ Use the `aex-bootstrap` command or individual components. For detailed steps, see Symantec Knowledge Base article HOWTO21645. See "Command-line options for managing Mac client computers" on page 35.
Step 6	On the Mac, check the agent installation.	See "Checking the agent installation" on page 34. After you install the agent, the managed Mac is ready to receive solution plug-ins. You are not required to install plug-ins as a separate step. Solutions install their plug-ins through policies. See "About solution plug-ins for Mac" on page 35.

Setting up Notification Server name resolution with Mac computers

A prerequisite for installing Symantec Management Agent on Mac client computers is to set up Notification Server name resolution.

See "Symantec Management Agent for Mac installation prerequisites" on page 21.

One way to set up name resolution is to add the Notification Server computer host name and IP address to the `/etc/hosts` file on the Mac client computer.

This task is a step in the process for installing the Symantec Management Agent on Mac client computers.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To set up Notification Server name resolution with Mac computers

1. As an admin user, on the Mac client computer open Terminal.app.

   If you have opened a remote SSH session from Symantec Management Console, start this procedure with the next step.

2. At the command line, enter `sudo vi /etc/hosts`.
3. At the prompt, enter the current admin user's password.
4. When the file contents appear, press the Down-arrow key or the lowercase **j** key until you reach the last line of the document.
5. Press the lower-case letter **o** key to open a new line below the line that the cursor is on.

   This action opens the **insert/edit**mode.
6. On the new line in the **insert/edit** mode, enter the Notification Server computer IP address and the Fully Qualified Domain Name (FQDN) of the Symantec Management Platform server.

   If you prefer, you can enter the short name or other alias for the Symantec Management Platform server on this same line.
7. Press **Esc** to exit **insert/edit** mode.
8. Press the **colon (:)** key.
9. At the **:** prompt at the bottom of the screen, enter the lowercase letters `wq` to write the file to disk and exit the vi editor.
10. At the shell prompt, enter `cat /etc/hosts` to review the entry that you added.

Note: If you need information about the vi editor or how to use it, you can find many sources of good information on the Web.

Disabling or configuring a built-in Mac OS X firewall

For a push installation to a Mac client computer, you must disable or configure the firewall. If you do not disable the firewall, you must configure it to allow incoming and outgoing connections to and from Symantec Management Console.

Caution: You must disable the firewall or configure it to allow communication with the console. Otherwise, you cannot install Symantec Management Agent and plug-ins.

This action is part of the process for installing the agent for Mac.

See "Process for installing Symantec Management Agent for Mac" on page 24.

The following information about ports and protocols is from Ports and Protocols for Symantec Management Platform 7.0.

Relevant information for configuring a Mac OS X firewall is shown in the following tables:

Table 2-3 Notification Server ports

Component	Port	Protocol
Notification Server	1024-65536 Default = 52028	TCP/IP
Notification Server	1024-65536 Default = 52029	TCP/IP Multicast
Agent	80	HTTP

Initial connection of Notification Server to client uses the following port:

- TCP 445 (MS DS/CIFS)

Initial connection of the client to Notification Server (after Service Starts) uses the following port:

- TCP 80 (HTTP) client download

Use the following ports for various services:

HTTP Client / Server communications, such as policy updates and posting events	The Agent establishes a connection to server port TCP 80 for HTTP and server port TCP 443 for SSL. This port is configurable by the user and can be set to any free port.
Downloading packages from Notification Server	Clients can download through HTTP.
Wake on LAN and Power Management	The default port is 52028.
To access Symantec Management Console using a remote computer	Notification Server uses HTTP (port 80) to connect to the server and download the client application or console content.

To communicate with Symantec Management Agent on the Mac	Notification Server uses SSH to connect to the client computer. Notification Server copies the bootstrap and then HTTP or HTTPs from the client computer to Notification Server to download the agent, as follows: ■ Initial connection of Notification Server to UNIX, Linux, or Mac client TCP 22 (SSH, configurable) ■ Initial connection of client to Notification Server (after Service Starts) TCP 80 (HTTP), 443 (HTTPS) or other custom port depending on Notification Server configuration for agent download

Disable or configure a built-in Mac OS X firewall for the version that you are running, as follows:

- Mac OS X 10.6 computer
  See "To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.6 computer" on page 30.
- Mac OS X 10.5 computer
  See "To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.5 computer" on page 31.
- Mac OS X 10.4 computer
  See "To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.4 computer" on page 31.

To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.6 computer

1. On the client Mac, on the **Apple** menu, click **System Preferences...**.
2. In the **System Preferences** window, on the **View** menu, click **Security**.
3. Click the **Firewall** tab.
4. Click **Start** to enable the firewall or click **Stop** to disable it.
5. To configure the firewall click **Advanced...**.

6 The following options appear:

Block all incoming connections	This option is the strictest one.
Automatically allow signed software to receive incoming connections	Lets digitally signed applications access your network without prompting
Enable stealth mode	Causes the computer to ignore pings and similar software that attempts to discover your computer
Plus (+) and minus (-) buttons	The buttons let you add applications to the firewall and remove applications from the firewall. When you add applications, you can either allow traffic to them or block traffic from them.

7 To save settings, click **OK**.

To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.5 computer

1 On the client Mac, on the **Apple** menu, click **System Preferences...**.

2 In the **System Preferences** window, on the **View** menu, click **Security**.

3 Click the **Firewall** tab.

4 To configure the firewall, at the top of the window click one of the following radio buttons:

Set access for specific services and applications	This option is the best one for most users. It blocks most incoming connections but lets you make exceptions for trusted services and applications.
Allow only essential services	Activates the firewall in its strictest mode.
Allow all incoming connections	Deactivates the firewall.

To disable or configure a built-in Mac OS X firewall on a Mac OS X 10.4 computer

1 On the client Mac, on the **Apple** menu, click **System Preferences...**.

2 In the **System Preferences** window, on the **View** menu, click **Sharing**.

3 Click the **Firewall** tab.

4. Click **Start** to activate the firewall or click **Stop** to deactivate it.
5. (Optional) Under the **Services** and **Firewall** tabs, check the boxes for the services that you want to enable.

   You can enable some incoming connections by making exceptions to the firewall. The firewall only blocks incoming connections from other computers, so you do not need to enable ports for services on other computers that you want to access.

   For example, you do not have to allow Personal Web Sharing to access other Web pages . If you cannot access a specific kind of online service, add a firewall exception for it. If the port or the service type that you want to offer is not in the list, you can add it. If you know the port number of the service, under the **Firewall** tab click **New...** and then click **Other**. Enter the port number and save changes.

Allowing incoming connections through SSH

After you have either disabled or configured the firewall to allow incoming and outgoing communication, you must verify connections.

Specifically, you must verify that the Mac OS X computer allows incoming connections through the SSH protocol. The Apple Mac OS X operating system has SSH installed by default, but the SSH daemon is not enabled automatically. This means that a user cannot log in remotely until you enable it.

This action is part of the process for installing the agent for Mac.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To allow incoming connections through SSH

1. On the client Mac, in **System Preferences**, under **Internet & Networking**, click **Sharing**.
2. In the list that appears, check **Remote Login**.
3. The SSH daemon starts immediately, and you can log in remotely using your user name.

   The **Sharing** window shows the name and IP address to use. You can also find this information by entering the following commands at the Terminal:

   `whoami` and `ifconfig`

Note: If the Mac client is located some distance from the platform server where you normally work, you have an alternative. You can work through an SSH session with the client Mac after you enable the SSH connection. You can use any SSH connection tool to enable and establish an SSH connection. One such tool is PuTTY. You can then perform actions on the Mac client computer through the SSH session instead of from the Mac terminal.

Installing Symantec Management Agent to the Mac OS X client computer

Deploying Symantec Management Agent is prerequisite to installing the Inventory Solution plug-in or deploying Inventory policies.

This task is a step in the process for installing the agent for Mac.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To deploy the Symantec Management Agent to the Mac OS X computer

1. In Symantec Management Console navigate to **Actions > Agents/Plug-ins > Push Symantec Management Agent**.
2. Click **Install Agent for UNIX, Linux and Mac**.
3. In the text field, enter the host name or IP address and click **Add**.
4. Select the computer that you added, and click **Installation Settings**.

5 In the **Privileged account password** field, enter the root account password for the Mac and ensure that the remaining settings are correct.

Note that the installation directory settings under **Agent Settings** do not apply to Mac OS X.

Note: If you have not configured the root user account, enter the administrator account credentials. If you have configured the root user account, enter the administrator account credentials. Enter the credentials in the **Unprivileged** user field and insert the root user credentials in the **Privileged** account field.

---

6 Click **OK** to save settings.

7 After the **Install Settings** window closes, click **Install** to begin installing the Symantec Management Agent to the Mac OS X computer, and confirm your choice.

8 Wait one minute to allow the agent to install.

9 On the Mac OS X computer click **Go > Utilities** to verify that the Symantec Management Agent icon is present.

10 Click **Go > Utilities > Terminal** and enter one of the following commands to check the log file:

- `aex-helper check`
- `aex-helper query ns`
- `aex-helper -v`
- `aex-sendbasicinv`

You can run terminal commands on the physical client computer, or you can perform this step through an SSH session with the Mac client.

11 Ensure that no errors exist in the log file.

Checking the agent installation

Ensure that the agent was installed correctly.

This task is a step in the process for installing the agent on Mac client computers.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To check the agent installation

1. On the Mac OS X computer click **Go > Utilities** to verify that the Symantec Management Agent icon is present.
2. Click **Go > Utilities > Terminal** and enter the following command to check the log file:

   ```
   less /opt/altiris/notification/nsagent/aex-nsclt-install.log
   ```

   You can run terminal commands on the physical client computer, or you can perform this step through an SSH session with the Mac client.
3. Ensure that no errors exist in the log file.

About solution plug-ins for Mac

In most cases you only install Symantec Management Agent. After you install Symantec Management Agent, you enable installation policies for solutions from the console as you do with Windows computers. After that the agent on the managed Mac checks policies, and any required solution plug-ins are installed automatically. Some solution plug-ins are installed automatically through Symantec Management Agent.

See "Process for installing Symantec Management Agent for Mac" on page 24.

In some cases you install a plug-in. These cases are called out explicitly in the text of solution-specific documentation when you are required to install a plug-in.

Plug-in policies come with a default target (or filter) for Mac computers. You can change targets; for example, if some Mac computers on your network are servers, you can exclude them from having solution plug-ins installed.

You can download required plug-in such as plug-ins for Inventory Solution, Patch Management Solution, and Software Management Solution from Notification Server, which you access in Symantec Management Console. If you have Notification Server and site servers, the agent on the managed Mac detects the nearest and fastest server and downloads plug-ins from there.

Command-line options for managing Mac client computers

When managing Mac client computers in Altiris Client Management Suite 7.1 from Symantec, you may need to use command-line options.

See "Process for installing Symantec Management Agent for Mac" on page 24.

You can view a list of command-line options by executing the following commands at the Mac Terminal or through an SSH remote connection:

See "About the Mac Terminal and Secure Shell (SSH)" on page 20.

- `-h`
- `-help`

Refer to the following technical articles for details about how to use command-line options when you manage Mac client computers:

- TECH29115 titled "NS Agent for UNIX, Linux, and Macintosh commands and command-line parameters."
  This article presents all user-facing commands. This article was written for 6.x; however, most information applies to 7.x.
- TECH45453, titled "Client Task Agent 7.x for UNIX, Linux, and Macintosh command lines." Includes the `aex-cta` command.
- HOWTO36005, titled "UNIX, Linus, and Macintosh aex-smf command-line tool."
  This tool is new in 7.1.

About selecting Mac computers for a Symantec Management Agent manual installation

Before you can manually install the Symantec Management Agent from the **Symantec Management Agent Install** page, you need to enter or select the appropriate computers. You can select the computers that have been discovered with Network Discovery. If you prefer, you can enter the computer names manually or import the computers through Active Directory or from a .csv file.

See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 37.

The .csv file is a comma-separated value (comma-delimited) text file. The file includes the DNS names or the IP addresses and administrator credentials of the client computers on which you want to install Symantec Management Agent. A template for the .csv file is located in the UNIX/Linux/Mac push installation screen.

For Mac computers, each line in the .csv file represents a computer entry that is imported into the **Symantec Management Agent Install** page. You can also include the appropriate installation settings in the .csv file. These installation settings let you configure the communication and the authentication settings for the Symantec Management Agent for Mac.

Note: If you have a large number of computers that require different connection and configuration settings, use a .csv file to import the computers.

See "Creating a .csv file for importing Mac computers" on page 38.

Selecting Mac computers for a Symantec Management Agent pull installation

You can select Mac computers for a manual Symantec Management Agent installation. With this type of installation, you download files and execute them on the client computer.

See "About selecting Mac computers for a Symantec Management Agent manual installation" on page 36.

This task is a step in the process for installing the Symantec Management Agent on Mac client computers.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To select Mac computers for a Symantec Management Agent manual installation

1. In Symantec Management Console, click **Settings > Agents/Plug-ins > Symantec Management Agent > Settings > Install agent for UNIX, Linux, Mac** .
2. Highlight the computers to which you want to roll out the agent, as follows:

To manually add a computer	In the text box, type the computer name (which must be a DNS-resolvable name) or IP address and then click **Add**.
To select from the available computers	Click **Select Computers** and then, in the **Select Computers** window, select the appropriate computers.
To import computers from a .csv file	1 In the toolbar, click **Import computers from a selected file**. 2 In the **Select file to import** dialog, select the appropriate .csv file, and then click **Open** See "Creating a .csv file for importing Mac computers" on page 38.

   The selected computers are added to the list.
3. Click **Installation Settings**, and specify the settings:

4 Verify that each computer meets the Symantec Management Agent installation prerequisites.

See "Symantec Management Agent for Mac installation prerequisites" on page 21.

5 If you want to remove a computer from the list, select it in the list and then click **Remove Computer**.

Creating a .csv file for importing Mac computers

If you want to install the Symantec Management Agent for Mac on a large number of computers, Symantec recommends that you use a .csv file. When you install the agent on the computers that require different connection and configuration settings, it is simpler to use a .csv file. Use a .csv file to import the computers and configure the installation settings.

The .csv file is a comma-delimited text file. This file includes the DNS names or the IP addresses of the client computers on which you want to install the Symantec Management Agent. Each line in the .csv file represents a computer entry that is imported into the **Symantec Management Agent Install** page. The .csv file can also contain the installation settings for each computer.

See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 37.

See "Installing the Symantec Management Agent for Mac with a push" on page 41.

A .csv template file for importing UNIX, Linux, and Mac computers (`CSVTemplate.csv`) is provided with the Symantec Management Platform. The column header of the .csv template indicates the data that is required and the valid values that you can use.

Warning: The .csv file format (list separator) must meet the regional settings of the server. For example, the sample `CSVTemplate.csv` file uses the "English (United States)" regional settings with a comma "," as a list separator. You can view the Symantec Management Platform's regional settings in the Windows **Control Panel**, under **Regional and Language Options**.

This procedure is a step in the process for installing the agent and plug-in for Mac.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To create a .csv file for importing UNIX, Linux, and Mac computers

1. In the Symantec Management Console, click **Settings > Agents/Plug-ins > Symantec Management Agent > Settings**.
2. Double-click the **Symantec Management Agent Install** page, and click the **Install Agent for UNIX, Linux and Mac** tab.
3. In the **Rollout Agent for UNIX, Linux and Mac to Computers** pane, right-click **CSV file template**, and then click **Save Target As**.
4. In the **Save As** dialog box, save the `CSVTemplate.csv` file in the appropriate location under a suitable name.
5. Open the new .csv file in a text editor. Enter the information for each computer on which you want to install the Symantec Management Agent for UNIX, Linux, and Mac.

   You do not have to use all of the fields. You can use only the fields that you need, such as computer name, admin name, admin password, and so on.

   The settings that you can specify in the .csv file are identical to the settings that you can set from the **Install Settings** window in Symantec Management Console.

   See "Installation Settings dialog box" on page 45.
6. When you have finished, save the .csv file.

About installing the Symantec Management Agent for Mac with a push

The Symantec Management Platform computer pushes the installation of the Symantec Management Agent for Mac.

See "Installing the Symantec Management Agent for Mac with a push" on page 41.

Table 2-4 Overview of the Symantec Management Agent for Mac push installation process

Step	Description
Step 1	Symantec Management Platform attempts to connect to the target computer through SSH. The SSH protocol supports logon with either privileged or unprivileged user accounts and multiple passwords. A privileged user has more access than an unprivileged user. Therefore, it is more secure to connect through unprivileged users. This step refers to connecting from Symantec Management Console to the client Mac through SSH. Symantec assumes that the client is configured not to allow a privileged SSH user to connect remotely. If you use unprivileged users, you must also specify at least one privileged user. You must use a privileged account to install the agent. See "Symantec Management Agent for Mac installation prerequisites" on page 21.
Step 2	When a connection is established, Symantec Management Platform determines the client computer's operating system and environment. The platform then launches the appropriate platform-specific push-install script.
Step 3	The push-install script creates a directory structure on the client computer. It then attempts to download the `aex-bootstrap` utility from the Symantec Management Platform computer. The push-install script tries each of the following methods, in order, until one succeeds: SCP/SFTP, wget, curl. If all of these methods fail, the script uses `dd` command to transfer the `aex-bootstrap.Z.uu` archive to the target computer. It then uses uudecode to convert the archive to a native format.
Step 4	The `.aex-agent-install-config.xml` file, which contains all of the Symantec Management Agent installation settings, is downloaded to the client computer.
Step 5	The `aex-bootstrap` script is executed, and the SSH connection to Symantec Management Platform is closed.
Step 6	The `aex-bootstrap` script downloads the rest of the Symantec Management Agent from the Symantec Management Platform computer. It then configures the Symantec Management Agent with settings from the `.aex-agent-install-config.xml` file.
Step 7	When the Symantec Management Agent for Mac runs for the first time, it collects basic inventory and posts it to Symantec Management Platform.
Step 8	After all necessary updates are completed on the platform server, Symantec Management Agent for Mac receives tasks and policies from Symantec Management Platform.

Installing the Symantec Management Agent for Mac with a push

You can push the Symantec Management Agent for Mac to any computer that is listed in the **Symantec Management Agent Install** page.

The Symantec Management Platform computer performs the push installation of the Symantec Management Agent for Mac. The Symantec Management Platform computer establishes a connection to the target Mac computer and uploads the required files. It then executes the files on the target computer.

See "About installing the Symantec Management Agent for Mac with a push" on page 39.

This task is a step in the process for installing the Symantec Management Agent on a Mac OS X computer.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To install the Symantec Management Agent for Mac with a push

1. Select the Mac computers on which to install the Symantec Management Agent.

   You can select multiple computers by using the Shift or Ctrl key.

   See "Selecting Mac computers for a Symantec Management Agent pull installation" on page 37.

2. If necessary, configure the appropriate installation settings.

   If you added computers manually, you must specify the appropriate installation settings for each target computer before you install the Symantec Management Agent for Mac. If you imported computers from a .csv file, you may have specified the installation settings for each computer in that file. You can change these settings for individual computers or groups of computers.

   If you configured Mac computers in the same way, such as using the same password for the root account, you can select multiple computers using the Shift or Ctrl key. When you multiselect Mac computers, you only need to define Installation Settings once. Those settings apply to all previously selected Mac computers.

   See "Specifying the Symantec Management Agent for Mac installation settings" on page 44.

3 (Optional) In the **Simultaneous Tasks** box, specify the number of installations to run simultaneously.

This value defines the number of threads running in parallel and serving Symantec Management Agent pushing. All of the threads share a common queue from which they take the next computer to install to. The default value is 5, but you may want to use a different value. You might change the value to suit the performance of the Symantec Management Platform, the client computers, and the network capacity. Increasing the number of simultaneous tasks may reduce the total installation time.

4 Click **Install**.

The Status column in the computer list shows the success or failure of the installation on each computer. Note that the newly installed Symantec Management Agent reports its status back to the originating Notification Server. This reporting to the originating Notification Server occurs even if a different Notification Server manages the managed computer.

5 If the computer list is not refreshed automatically, in the toolbar, click **Refresh** to view the current push installation status for each computer.

6 When the installation process is complete, view the **Installation Status** report to confirm that the agent has been installed successfully on all of the computers

The installation process can take up to 10 minutes.

About installing the agent for Mac with a pull

Some Mac administrators prefer not to give anyone else access to their computers. Instead, they use a manual installation with `bootstrap` rather than a push from the console.

See "Process for installing Symantec Management Agent for Mac" on page 24.

If Mac clients do not have the utilities available to download `bootstrap`, or if Notification Server is unavailable for a push, you can use a manual installation.

Neither SSH nor Notification Server console is required for this type of installation.

See "Installing the Symantec Management Agent for Mac with a pull" on page 43.

Installing the Symantec Management Agent for Mac with a pull

You can pull the Symantec Management Agent to each computer if necessary. To pull the agent you must have a direct connection between Symantec Management Platform and the Mac client computer. The Notification Server computer component of Symantec Management Platform must be available through a direct, not a remote, connection with the Mac.

You might need to pull the agent in the following situations:

- SSH is not available.
- The target computers are behind a firewall.

See "About installing the agent for Mac with a pull" on page 42.

The `bootstrap` program always downloads from Notification Server. This installation includes the download of the agent and its components and occurs from Notification Server. The agent directory contains the agent components such as task handlers. The agent installation directory contains the bootstrap binary (executable) file.

The URL of the **Download Symantec Management Agent for UNIX, Linux and Mac** page is shown on the **Symantec Management Agent Install** page, in the **Download Page URL** panel. You can view the page, but you cannot change this setting.

This task is a step in the process for installing the Symantec Management Agent on a Mac OS X computer.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To preview the Download Symantec Management Agent for UNIX, Linux and Mac page

1. In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
2. On the **Symantec Management Agent Install** page, click the **Install Symantec Management Agent for UNIX, Linux and Mac** tab.
3. In the **Download Page URL for UNIX, Linux, and Mac users** pane, in the **Select platform** box, select the appropriate platform.
4. Click **View page**.

To pull the Symantec Management Agent for Mac to a remote computer

1. Log on to the remote computer as an administrator.
2. Ensure that the remote computer meets the Symantec Management Agent for Mac installation prerequisites.

   See "Symantec Management Agent for Mac installation prerequisites" on page 21.
3. On the remote computer, open a Web browser , and then go to the following URL:

   http://*SMPName*/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=*Platform*

   where *SMPName* is the name of your Symantec Management Platform computer and *Platform* is Mac.
4. Follow the instructions that are displayed on the **Download Symantec Management Agent for UNIX, Linux and Mac** page for downloading and running the install bootstrap program on the remote computer.

Specifying the Symantec Management Agent for Mac installation settings

The Symantec Management Agent installation settings are the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. You must specify the appropriate privileged account login name and password for each target computer.

See "Installing the Symantec Management Agent for Mac with a push" on page 41.

When you import computers from a .csv file, you can specify the appropriate installation settings for each computer in the .csv file. If you do not specify any settings in the .csv file, you must specify the appropriate settings for each target computer. You must also specify the appropriate settings for each computer if you added computers manually, Specify those settings before you install the Symantec Management Agent for Mac.

You can specify installation settings for a particular computer or for multiple computers. If you select multiple computers, the same installation settings are applied to each computer. You can also clone the current installation settings from a computer and apply it to other computers.

See "Creating a .csv file for importing Mac computers" on page 38.

This task is a step in the process for installing the Symantec Management Agent on Mac client computers.

See "Process for installing Symantec Management Agent for Mac" on page 24.

To specify the Symantec Management Agent installation settings

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
2. On the **Symantec Management Agent Install** page, click the **Install Symantec Management Agent for UNIX, Linux and Mac** tab.
3. Under **Rollout Agent for UNIX, Linux, and Mac to Computers**, in the computer list, select the computer for which you want to change the Symantec Management Agent installation settings.

   If you want to specify identical installation settings for multiple computers, select the appropriate computers.
4. Click **Installation settings**.
5. (Optional) If you want to clone the current installation settings from a particular computer, in the **Installation Settings** dialog box, in the **Load settings of** drop-down list, select the appropriate computer.
6. Specify the appropriate installation settings for the selected computers.

   See "Installation Settings dialog box" on page 45.
7. When you have finished, in the **Installation Settings** dialog box, click **OK**.

Installation Settings dialog box

When you click the button on the Push Install screen in the console you see the **Installation Settings** dialog box.

The **Installation Settings** dialog box lets you configure the Symantec Management Agent for UNIX, Linux, and Mac push installation settings.

In the **Installation Settings** dialog box, the name of the computer that you selected in the **Symantec Management Agent Install** page is displayed in the **Applies to** line. If you selected multiple computers, the number of selected computers is displayed.

If you have selected multiple computers, the option **Load settings of** appears. This drop-down list lets you select the computer from which to clone the current installation settings. The cloned settings are applied to all the computers that you selected in the **Symantec Management Agent Install** page.

See "Specifying the Symantec Management Agent for Mac installation settings" on page 44.

Table 2-5 Tabs on the **Installation Settings** dialog box

Tab	Description
Connection and Authentication	This tab lets you configure the communication and the authentication settings for the Symantec Management Agent for Mac push installation. See "Installation Settings: Connection and Authentication tab" on page 46.
Agent Settings	This tab lets you configure the Symantec Management Agent for Mac upgrade, configuration, and startup settings. See "Installation Settings: Agent Settings tab for Mac computers" on page 51.
Install XML	This tab displays the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format. You can save the XML to a file and upload the file to a client computer. Then you can use it to manually install and configure the Symantec Management Agent for Mac. See "Installation Settings: Install XML tab" on page 52.

Installation Settings: Connection and Authentication tab

The **Connection and Authentication** tab lets you configure the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac push installation.

See "Installation Settings dialog box" on page 45.

Warning: Do not use non-ASCII characters in file or directory names when you configure installation settings.

On the client side, SSH must allow the certificate connection, where by default only user name and password are used. The procedure for generating an SSH key is beyond the scope of this guide.

Table 2-6 Installation Settings: Connection and Authentication tab

Setting	Description
Try connect via SSH using SSH Key authorization	When you enable this option, these settings are used to establish an SSH connection to the target Mac computer using SSH key authorization. See "Try connect by SSH using SSH Key authorization settings" on page 47.

Table 2-6 Installation Settings: Connection and Authentication tab *(continued)*

Setting	Description
Try connect via SSH using password authorization	When you enable this option, these settings are used to establish an SSH connection to the target Mac computer. The connection is established with SSH password authorization. See "Try connect by SSH using password authorization settings" on page 48.
Login and password	These settings specify the appropriate user account credentials for SSH connections. See "Login and password settings" on page 48.
Timeout settings	These settings specify the login timeout periods and command timeout periods and the upload speed of the Symantec Management Agent package. See "Timeout settings" on page 50.
Platform detection	These settings specify whether Symantec Management Platform automatically detects the target computer's operating system or whether the target computer's operating system is defined manually. See "Platform detection settings" on page 51.

Try connect by SSH using SSH Key authorization settings

These settings are used to establish an SSH connection to the target UNIX, Linux, or Mac computer using SSH key authorization. The SSH key authorization method lets you connect to the target computer from an authorized computer without entering a user name and a password.

To use SSH key authorization, you first need to generate an SSH key. You then need to save the SSH private key on the Symantec Management Platform computer, and configure the target computer with the SSH public key. To generate an SSH key, you can use a native SSH key generator. You can also use the SSH key generation module that is provided with Symantec Management Platform.

See "Installation Settings: Connection and Authentication tab" on page 46.

Table 2-7 Try connect by SSH using SSH Key authorization settings

Setting	Description
SSH key file	The SSH private key file to use. You can type the full path and file name, or click **...** to select the appropriate file.
SSH key password	The password that is used to protect the SSH key file. If no password is configured, leave this field blank.

Table 2-7 Try connect by SSH using SSH Key authorization settings *(continued)*

Setting	Description
SSH key type	The type of SSH key encoding: RSA or DSA.
Port	The port to which the target computer's SSH server listens. Default: 22
Prompt	The target computer's logon prompt for a privileged user. Default: `%, $, #, >`

Try connect by SSH using password authorization settings

This setting specifies the port to use when the Symantec Management Platform attempts to connect to the target computer using SSH password authorization.

See "Installation Settings: Connection and Authentication tab" on page 46.

Table 2-8 Try connect by SSH using password authorization settings

Setting	Description
SSH port	The port to which target computer's SSH server listens. Default: 22

Login and password settings

These settings specify the appropriate privileged user account credentials for SSH connections. You can optionally specify multiple privileged user accounts and unprivileged user account credentials.

See "Installation Settings: Connection and Authentication tab" on page 46.

Table 2-9 Login and password settings

Setting	Description
Privileged account login	The login name of a privileged user account. A privileged user is one that has permission to install and use system programs. Default: root.
Privileged account password	The password for the privileged user account that was specified previously.

Table 2-9 Login and password settings *(continued)*

Setting	Description
Privileged account prompt	The target computer's logon prompt for a privileged user. Separate multiple values with a comma. Default: %, $, #
Use privileged account multiple password	This option lets you install the Symantec Management Agent on a group of computers that have different privileged user account names and passwords. The specified login name and password combinations are tried on each target computer until the connection succeeds. **Warning:** The passwords that you type in this section are not hidden. You need to specify the following information: ■ **Logins**: The list of privileged account login names, one entry per line. ■ **Passwords**: The corresponding list of privileged account login passwords, one entry per line. ■ **Prompts**: The target computer's logon prompt for a privileged user. Separate multiple values with a comma. Default: %, $, #
Log in first using unprivileged user	This option lets you log in with an unprivileged (unauthorized) user account first. You then switch to a privileged user account. You can use this option if the target computer does not allow remote privileged user logons. Specify unauthorized user credentials or enter multiple users and passwords. You need to specify the following information: ■ **Unprivileged User Login**: The login name of an unprivileged user account. ■ **Unprivileged User Password**: The password for the privileged user account that is specified previously. ■ **Unprivileged User Prompt**: The target computer's logon prompt for an unprivileged user. Separate multiple values with a comma. Default: `%, $, #, >` **Note:** A regular unprivileged user on Mac OS X must be given permissions to SSH to the system. Otherwise, the unprivileged user may not have SSH access to the Mac OS X system to perform push install. To supply the user with SSH access, on Mac OS X go to **System Preferences > Sharing > Remote Login**. A regular unprivileged user on Mac OS X can only be used to perform a push installation through users who are allowed to administer the computer. On Mac OS X, see **System Preferences > Accounts**. Due to the implemented security on Mac OS X, unprivileged users cannot use root user to perform a push installation.

Table 2-9 Login and password settings *(continued)*

Setting	Description
Use unprivileged user multiple passwords	This option lets you install the Symantec Management Agent on a group of computers that have different unprivileged user account names and passwords. The specified login name and password combinations are tried on each target computer until the connection succeeds. **Warning:** The passwords that you type in this section are not hidden. You need to specify the following information: ■ **Logins**: The list of unprivileged account login names, one entry per line. ■ **Passwords**: The corresponding list of unprivileged account login passwords, one entry per line. ■ **Prompts**: The target computer's logon prompt for an unprivileged user. Separate multiple values with a comma. Default: `%, $, #, >`

Timeout settings

These settings specify the login timeout periods and the command timeout periods and the upload speed of the Symantec Management Agent package.

See "Installation Settings: Connection and Authentication tab" on page 46.

Table 2-10 Timeout settings

Setting	Description
Login timeout	Specifies how long the Symantec Management Platform should wait for a successful login to the target computer. Default: 120 seconds
Command timeout	Specifies how long the Symantec Management Platform should wait for a reply from the commands that are executed during the push installation. Default: 60 seconds
Upload speed	Specifies the upload speed of the Symantec Management Agent installation package. The available values are Fast, Medium, Slow. This option affects uploading with the dd command only. See "About installing the Symantec Management Agent for Mac with a push" on page 39.

Platform detection settings

These settings specify whether the Symantec Management Platform automatically detects the target computer's operating system or whether the target computer's operating system is defined manually. If the target computer's operating system is defined manually, you need to select the appropriate value.

See "Installation Settings: Connection and Authentication tab" on page 46.

Warning: Be careful with the manual selection option if you want to configure installation settings for multiple computers.

Table 2-11 Platform detection settings

Setting	Description
Automatically discover OS type	The Symantec Management Platform detects the target computer's operating system automatically when the push installation process starts.
Manually select OS type	This drop-down list specifies the target computer operating system.

Installation Settings: Agent Settings tab for Mac computers

On the **Agent Configuration** page, the **Agent settings** tab lets you configure the Symantec Management Agent for Mac upgrade, configuration, and startup settings. If you need to upgrade the Symantec Management Agent from an earlier version, you can choose to keep the current Symantec Management Agent settings. The Directories settings specify the directories that the Symantec Management Agent uses. The Symantec Management Agent execution settings define the behavior of the Symantec Management Agent during and after installation.

See "Installation Settings dialog box" on page 45.

Warning: Do not use non-ASCII characters in file or directory names when you configure installation settings.

Table 2-12 Installation Settings: Agent settings tab

Setting	Description
Keep the current Agent settings if possible	If you need to upgrade the Symantec Management Agent from an earlier version, this option preserves the current Symantec Management Agent settings where applicable. Disable this option if you want to reinstall the Symantec Management Agent and configure it with the installation settings that you specify on this tab.
Installation directory	The directory where the Symantec Management Agent is installed. Default: /opt/altiris/notification/nsagent **Note:** On Macintosh, the Symantec Management Agent is always installed into the default directory.
Links directory	The directory where links to the Symantec Management Agent's executable binaries are placed. Default: /usr/bin
Directory for packages	The directory to which software delivery policies and tasks download packages. Default: %INSTDIR%/var/packages
Run Agent for Mac on startup	Specifies that the Symantec Management Agent is to run in the background each time the Macintosh computer starts. This setting is the default. If this setting is disabled, you must restart the agent manually every time you start the Mac client computer.
Start the Agent after installation	Specifies that the Symantec Management Agent is to start immediately after the push installation. If you disable this setting, the agent starts automatically after the next reboot, but only if the **Run Agent for Mac on startup** setting is enabled.
Allow unprivileged users to run programs	Specifies that unauthorized users are allowed to run software delivery policies and tasks on the target computer.

Installation Settings: Install XML tab

The **Install XML** tab displays the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format. You can save the XML to a file and upload the file to a client computer. You then use the file to manually install and configure the Symantec Management Agent for Mac.

If you use `aex-bootstrap` for manual agent installation, the `aex-bootstrap` looks for this XML file in the **/tmp** directory. To facilitate that process, copy the XML

file as `.aex-agent-install-config.xml` to the **/tmp** directory. You can then run `aex-bootstrap` manually to use the settings that this file contains. The XML file settings override any `aex-bootstrap` command line parameters, including the specification of the Notification Server computer name.

See "Installation Settings dialog box" on page 45.

Table 2-13 Installation Settings: Install XML tab

Setting	Description
Main display area	The main display area shows the Symantec Management Agent for Mac upgrade, configuration, and startup settings in XML format.
Save as file	This button lets you save the displayed XML to a file.

About the Mac firewall and digitally signed packages

Digital signatures are not currently available for the Mac firewall.

See "Symantec Management Agent for Mac installation prerequisites" on page 21.

Note that if you have an enterprise firewall and have the software firewall disabled, then the following scenario is not a problem. Otherwise, the following scenario can occur. An application such as iTunes is signed by a valid certificate authority and runs on a Mac computer in your environment. The application is added automatically to the list of allowed applications. In this case, users are not prompted to authorize the applications. Other applications cannot receive information through the firewall.

Refer to the following resources for information about the Mac OS X application firewall:

- Apple Support site
- Symantec Knowledge Base articles "Installing the Symantec Management Agent for Mac with the firewall enabled" and "What is the /delaystart option and how should it be configured".

Chapter 3

Configuring the Symantec Management Agent for Mac

This chapter includes the following topics:

- About configuring the Symantec Management Agent for Mac
- Configuring the global agent settings
- Configuring the targeted agent settings on Mac computers
- About maintenance windows for managed computers
- Configuring maintenance window policies

About configuring the Symantec Management Agent for Mac

The default Symantec Management Agent configuration settings are suitable for a small Symantec Management Platform environment, such as fewer than 1,000 nodes.

As your environment grows, or if your organization has particular requirements, you need to make the appropriate configuration changes.

The agent configuration settings are applied to the appropriate managed computers using agent configuration policies. You can modify these policies to change the settings at any time. The new configuration settings are applied to the agents when the managed computers get their next policy updates (which is typically once a day).

The Symantec Management Platform provides the following types of agent configuration policies:

Global settings	The global configuration settings apply to all Symantec Management Agents on all managed computers. These settings are applied as a single policy that automatically targets every managed computer. See "Configuring the global agent settings" on page 56.
Targeted settings	The targeted agent settings are the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can modify the default policies that are supplied with the Symantec Management Platform. You can create your own targeted agent settings policies and apply them to the appropriate managed computers. See "Configuring the targeted agent settings on Mac computers" on page 61.
Maintenance windows	A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance window policy defines one or more maintenance windows. You can modify the default policy that is supplied with the Symantec Management Platform. You can create your own maintenance window policies and apply them to the appropriate managed computers. See "About maintenance windows for managed computers" on page 73.

The targeted settings policies and maintenance window policies are applied to the managed computers that are included in the specified policy targets. These targets may not be mutually exclusive. Two or more policies of the same type may apply to the same managed computer.

If a managed computer has two or more targeted settings policies that are applied to it, Notification Server selects the policy to use. The selection is based on the policy GUID, and is not transparent to the user. You cannot determine beforehand which policy is chosen. However, once the selection has been made, it is used consistently to ensure that the same policy is applied at every policy update.

If two or more maintenance window policies apply to the same managed computer, the policies are merged. All of the specified maintenance windows are used.

Configuring the global agent settings

The global configuration settings are set the same way on all computers. These settings apply to all Symantec Management Agents on all managed computers. The global agent settings are applied as a global agent settings policy, so they are updated in the same way as any other policy. By default, the global agent settings

policy is refreshed hourly. You cannot delete or disable the global agent settings policy or create alternative versions of it.

If you want to specify agent settings for particular groups of managed computers, you need to configure the appropriate targeted agent settings policies.

See "Configuring the targeted agent settings on Mac computers" on page 61.

To configure the global agent settings

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Global Settings**.
2. Make the appropriate configuration settings on the following tabs:

General	Specify the Tickle/Power Management and Package Multicast settings. See "Symantec Management Agent Settings – Global: General tab" on page 57.
Authentication	Specify the user name and password that the Symantec Management Agent uses when it connects to Notification Server or a package server. See "Symantec Management Agent Settings – Global: Authentication tab" on page 60.
Events	Specify Notification Server events that you want to capture.

3. Click **Save Changes**.

Symantec Management Agent Settings – Global: General tab

The **General** tab contains the Tickle/Power Management settings and the Package Multicast settings.

The Tickle/Power Management settings are the TCP/IP Port numbers and IP addresses, which the Symantec Management Agents use to communicate with the Power Management tool.

Table 3-1 Tickle/Power Management settings

Setting	Description
TCP/IP port	The TCP/IP Port number must be between 1024 and 65535. The default is port 52028.

Table 3-1 Tickle/Power Management settings *(continued)*

Setting	Description
TCP/IP multicast address	The IP address that the Symantec Management Agents use to listen to multicast Power Management commands on the network. The TCP/IP Multicast Addresses should be between 224.0.0.1 and 239.255.255.254. The last octet should not be 255. The default IP address is 224.0.255.135.
TCP/IP multicast port	The port number that the Symantec Management Agents use to listen to Power Management messages on the network. The TCP/IP Multicast Port number must be between 1024 and 65535. The default is port 52029.

The Package Multicast settings are the IP addresses, which the Symantec Management Agents use for multicasting.

Table 3-2 Package Multicast settings

Setting	Description
TCP/IP multicast address	The IP address that the Symantec Management Agents use to listen to multicast negotiation messages on the network. The default IP address is 224.0.255.135.
TCP/IP multicast port	The port number that the Symantec Management Agents use to listen to multicast messages on the network. The TCP/IP multicast port number must be between 1024 and 65535. The default port is 52030.
TCP/IP Listener range	The range of IP addresses from which a multicast session chooses to use during the multicasting of the package by the master. You can add new ranges, and specify the appropriate IP addresses for each range.
TCP/IP Exclusion range	The range of IP addresses that cannot be used for multicasting. You can add new ranges, and specify the appropriate IP addresses for each range.

About the Tickle/Power Management settings

The Power Management tool lets Notification Server communicate directly with an Symantec Management Agent. Under normal working conditions, the agent

requests its targeted agent settings policies from Notification Server and then responds accordingly. With power management, Notification Server can contact the agent directly through a tickle, and instruct it to act immediately.

See "Configuring the global agent settings" on page 56.

See "Symantec Management Agent Settings – Global: General tab" on page 57.

Power management allows Notification Server to perform the following tasks:

Wake on LAN	Notification Server immediately sends a signal to turn on the managed computer if it is currently turned off . The managed computer must have a Wake on LAN-enabled network card, and Wake On LAN must be enabled in the managed computer's BIOS settings. If you tickle an agent, Notification Server starts the computer using Wake on LAN, and then waits five minutes before you send the tickle. This delay allows time for the managed computer to turn on.
Get Client configuration	Notification Server contacts the agent and instructs it to request its targeted agent settings immediately.
Send basic inventory	Notification Server contacts the agent and instructs it to send its basic inventory immediately.

When you perform power management on multiple computers in a single operation, only the Wake on LAN action works. For the other actions to work, you must supply a multicast address and port.

The subnet or the proxy computers (relay computers) are never pinged to determine whether they are alive. To determine the most suitable relay computers, data from the CMDB is evaluated to create a prioritized list of computers. For each subnet, Notification Servers are given the highest priority, followed by package servers. All other computers in that subnet have priority in the order in which they last communicated with Notification Server. The more recent the communication, the higher the priority. The computers on the list are tried in order of priority until communication with a relay computer is successful. The attempt stops after the first 50 computers have been tried without success.

Some solutions use power management to perform solution-specific functions. Consult the appropriate solution Help for information.

The Tickle/Power Management settings are relevant only when power management has been enabled on a managed computer. This setting is specified in the targeted agent settings policy.

See "Targeted Agent Settings: Advanced tab" on page 72.

About the Package Multicast settings

The Package Multicast settings are applied to a managed computer only if multicast is enabled in the appropriate targeted agent settings policy.

See "Symantec Management Agent Settings – Global: General tab" on page 57.

See "Targeted Agent Settings: Downloads tab" on page 67.

When you change these settings, be aware of the following:

- There must be at least one listener IP address range specified that cannot be deleted.
- The Exclusion IP address ranges can be a subset of Listener IP address ranges but not vice versa.

Symantec Management Agent Settings – Global: Authentication tab

The **Authentication** tab contains the Agent Connectivity Credential (ACC) settings. These settings consist of the user name and password that the Symantec Management Agent uses to connect to a secured resource. The package server also uses the Agent Connectivity Credential to add file-based security to download package files, if so configured. The credentials that you specify must be a known account on Notification Server and every package server.

See "Configuring the global agent settings" on page 56.

Table 3-3 Settings on the **Authentication** tab

Setting	Description
Use Application credentials	Use the application identity credentials that you specified on the **Processing** tab of the Server Settings page.
Use these credentials	Specify the appropriate ACC user name and password. This account usually has a lower level of rights than the Application Identity account, and is a dedicated account created for use on package servers. **Warning:** You cannot use special characters (any of the following: **~!#$%^&(){}**) in the user name or password. You may use only alphanumeric characters.

Symantec Management Agent Settings – Global: Events tab

The **Events** tab lets you enable or disable individual Notification Server event captures. We recommend that you leave the Notification Server computer **Event**

options enabled. However, if you have a large number of managed computers and receive unneeded events, you can disable them. You specify the Notification Server events that you want to capture by checking the appropriate boxes.

See "Configuring the global agent settings" on page 56.

Table 3-4 Settings on the **Events** tab

Setting	Description
AeX Client Logon	Sent when users log on and off a computer.
Agent Install Status	Sent during push and pull installs to keep track of how the install progresses.
AeX SWD Execution	Sent when a software management task is run.
AeX SWD Package	Sent when a package is modified or downloaded.
AeX SWD Status	Sends status information about the software management tasks that the Symantec Management Agent receives. For example, when a new task is received or existing tasks have been updated or disabled.

Configuring the targeted agent settings on Mac computers

The targeted agent settings policy lets you configure the general parameters that control the Symantec Management Agent. These parameters include how the agent communicates with Notification Server . You can apply these settings to particular groups of computers. For example, some groups of computers may have different purposes, or you may want to treat servers differently from other managed computers. You can modify the default policies that are supplied with Notification Server or create your own targeted agent settings policies.

See "About configuring the Symantec Management Agent for Mac" on page 55.

The targeted agent settings policies supplied with Notification Server are as follows:

- All desktop computers (excluding site servers)
- All site servers
- All Mac OS X servers

If you want to specify some configuration settings that apply to all Symantec Management Agents on all managed computers, configure the global agent settings policy.

See "Configuring the global agent settings" on page 56.

To configure the targeted agent settings

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the left pane, do one of the following:
   - To create a new targeted agent settings policy, click **Create New**.
   - To modify an existing targeted agent settings policy, select the appropriate policy.
3. To set or change the policy name, click **Rename**.

   In the **Rename Item** dialog box, type the new name, and then click **OK**.

4 In the right pane, make the appropriate configuration settings on the following tabs:

General	General settings include the policy download and inventory collection frequencies, and the computers, users, or resource targets to which the policy applies. See "Targeted Agent Settings: General tab" on page 64.
UNIX/Linux/Mac	If the Symantec Management Agent for Mac is installed, this tab is available and provides general settings for managed Mac computers. See "Targeted Agent Settings: UNIX/Linux/Mac tab" on page 65.
Downloads	Download settings control how each agent downloads packages during software deliveries. You can enable multicast downloads and configure multicast for both master sessions and client sessions. See "Targeted Agent Settings: Downloads tab" on page 67. You can override these settings for individual software delivery policies and tasks. For more information, see the topics about Software Management settings in the Software Management Solution Help.
Blockouts	Blockout periods are times when all communication between the agent and Notification Server is disabled. You can set up any number of blockout periods. See "Targeted Agent Settings: Blockouts tab" on page 70.
User Control	The user control settings are the options that affect what the user of the managed computer can see. See "Targeted Agent Settings: User Control tab" on page 72.
Advanced	Lets you specify an alternate URL that the Symantec Management Agent can use to access Notification Server, and turn on the power management feature. See "Targeted Agent Settings: Advanced tab" on page 72.

5 (Optional) To restore the policy to its default settings, click **Restore Defaults**.

6 Click **Save Changes**.

Targeted Agent Settings: General tab

The targeted agent general settings include the policy download and inventory collection frequencies, and whether to compress large events when you send them to Notification Server. You also need to specify the computers, users, or resource targets to which the targeted agent settings policy applies.

See "Configuring the targeted agent settings on Mac computers" on page ?.

Table 3-5 Settings on the **General** tab

Setting	Description
Download new configuration	The interval at which the Symantec Management Agent requests new policy information from Notification Server. The default and recommended interval is one hour. When you first set up your Notification Server, set this time to 1, 5, or 15 minutes. This setting lets you find out how Notification Server interacts with the Symantec Management Agents. This time should then be increased to suit the number of managed computers that you have.
Upload basic inventory	The interval at which the Symantec Management Agent sends basic inventory to Notification Server. The default interval is one day. You should adjust this value according to the number of managed computers in your organization.
Compress events over	Select this option to compress events when they are sent to Notification Server, and set the minimum size. The recommended minimum size is 200 KB, which is a compromise between bandwidth and CPU usage. The value you choose here is a trade-off between bandwidth usage and CPU usage on the server. For example, you may want to set a low value for the events that are sent from mobile computers. You can set a higher value for events on well-connected LAN computers.
Applies To	Displays the details of the resource targets, computers, or users to which the agent settings policy currently applies. You can set or change the policy target as appropriate.

Recommended Symantec Management Agent data update intervals

The Symantec Management Agent regularly sends basic inventory data to and receives agent configuration data from Notification Server. You can configure

the intervals for these updates. The more computers you manage, the less frequently you should update the data to reduce the load on Notification Server.

See "Configuring the targeted agent settings on Mac computers" on page 61.

Table 3-6 Recommended Symantec Management Agent data update intervals

Number of managed computers	Basic inventory	Configuration request
0 - 499	30 minutes	15 minutes
500 - 1999	eight hours	four hours
> 2000	24 hours	eight hours

Notification Server includes an automation policy that is called the Scalability Check policy. This policy automatically sends you an email message when the update intervals are lower than the recommended values. The Scalability Check policy saves you from regularly checking the update intervals as computers are added to or removed from your network. You can turn the Scalability Check policy on or off as necessary and set the appropriate schedule.

Targeted Agent Settings: UNIX/Linux/Mac tab

The **UNIX/Linux/Mac** tab lets you define the settings that apply to UNIX, Linux, and Mac computers in the targeted group of computers.

See "Configuring the targeted agent settings on Mac computers" on page 61.

Table 3-7 Settings on the **UNIX/Linux/Mac** tab

Setting	Description
Symantec log directory	The directory where the Agent log is written. Default: %INSTDIR%/var
Symantec log name	The name of the log file. Default: aex-client.log
Symantec log size	The maximum amount of disk space that the Agent log uses. Default: 1024 KB
Symantec logging level	The Agent log detail level: Error, Warning, Info. Default: Error

Table 3-7 Settings on the **UNIX/Linux/Mac** tab *(continued)*

Setting	Description
Syslog logging level	The system logging level: None, Error, Warning, Info. This option lets you specify whether the Symantec Management Agent should post messages to the system log and set the appropriate log level. Default: None
Enable NIC error	The Symantec Management Agent for UNIX, Linux, and Mac reports an error when the client computer's host name and IP address are different from that reported by DNS. The error is reported only if this setting is enabled. You can view the **NameServ Error** in Symantec Management Console. View this error in Resource Manager under **View > Inventory > Data Classes > Basic Inventory > AeX AC TCPIP data class > DNS Server 3**.
Enforce host certificate is in CA	When this option is enabled, the local certificate authority is used to validate the host for all HTTPS connections.
Name of the CA certificates file	Specifies the full path to the file containing one or more CA certificates in PEM (Base64 encoded) format.
Enforce hostname verification for HTTPS connection	The Symantec Management Agent communicates with a host using HTTPs only if that host's name matches the name in the host's certificate. The verification is done only if you enable this option.
Return the following information as computer name	Specifies which name the client computer reports as its computer name: DNS Name or Computer Name (the local computer name).
Return the following information as computer domain	Specifies what the client computer reports as its domain: Empty (an empty string) or DNS Domain (its DNS domain name).
Read computer DNS domain name from /etc/resolv.conf	When this option is enabled, the Symantec Management Platform reads the client computer's domain name from the `resolv.conf` file, instead of performing a host name lookup.
Software Delivery	The settings in this section specify the preferred values for each process priority level that software delivery tasks use.

Table 3-7 Settings on the **UNIX/Linux/Mac** tab *(continued)*

Setting	Description
Use proxy server for agent/server communication	When this option is enabled, the agent communicates with Notification Server by the specified proxy server. You can specify the following proxy server settings: ■ **Proxy server URL** ■ **Port number** ■ **Username** ■ **Password**

Targeted Agent Settings: Downloads tab

The **Downloads** tab lets you define the throttling settings and configure multicast settings.

See "Configuring the targeted agent settings on Mac computers" on page 61.

The tab contains the following groups of settings:

Throttling — Lets you define the throttling settings, which enable throttling of downloads to the agent and set the slow-connection threshold.
See Table 3-8

Throttling periods — Lets you create and modify the throttling periods that you want to use.
See Table 3-9

Multicast Configuration Settings — Lets you enable multicast downloads and configure multicast for both master session and client session.
See Table 3-10

Table 3-8 Throttling settings

Setting	Description
Use Bandwidth Throttling	Enables bandwidth throttling.
Only throttle when bandwidth is below	Specifies a slow-connection threshold. If the connection speed falls below the value that you specify, the bandwidth throttling settings that you specify are applied.

Table 3-9 Throttling Periods settings

Setting	Description
Add throttling period	You can specify any number of throttling periods. If two or more periods overlap, the lowest throttling value is used. For each throttling period, you can set the following: ■ Start time ■ Duration The start time and duration of the throttling period. ■ Value ■ Unit The amount of throttling, where the numerical value is either a percentage of the maximum download rate, or a specific download rate in KB/sec.
Delete	Deletes the selected throttling period from the list.
Time zone	The time zone to use for defining the throttling periods. The available time zones are as follows: ■ Use agent time The times are specified without time zone information, and are applied at the local time at each managed computer. Throttling periods start and end at different times depending on the time zones of the managed computers. ■ Use server time The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The throttling periods start simultaneously irrespective of time zones, and are compensated for daylight saving. This option ensures that throttling periods are always coordinated with the specified local time on the server where the policy is created. ■ Coordinate using UTC The times are specified with time zone information, where the time zone offset is 0. The throttling periods start simultaneously irrespective of time zones. Daylight savings time does not affect throttling periods.

Table 3-10 Multicast Configuration settings

Setting	Description
By default the Symantec Management Agent should use multicast when it downloads packages	If multicast is set as the default for downloading packages in the Global Agent Settings policy, this option lets you turn it off. However, individual packages may override this setting. If the Global Agent Settings policy has multicast turned off, you cannot turn it on with this option.

Table 3-10 Multicast Configuration settings *(continued)*

Setting	Description
Maximum master sessions per computer	The maximum number of concurrent sessions for which a Symantec Management Agent can be the master. The default value is 2 for new policies and for most of the default targeted agent settings policies that are supplied with Notification Server. The exception is the All package servers policy, which has a default value of 10. This value is the suggested default for package servers.
Minimum receiving computers per session	The minimum number of Symantec Management Agents (excluding the master) that must join the session before package multicasting can proceed.
Wait time to begin session	The maximum time to wait for the minimum number of Symantec Management Agents (excluding the master) to join the session, before the session times out. This value can be defined as a percentage of the Download new configuration interval on the **General** tab, or in minutes. The default value is 50% of the Download new configuration interval. The larger the value, the more agents join the session and reduce bandwidth utilization on the local segment. However, it takes longer for the package to arrive. Configure this value higher than the minimum time to start multicast (around 10 minutes). If a session times out, the Symantec Management Agents that were members of the session attempts to download the package again through multicast. The agents continue this attempt until the **Maximum transmission attempts per package** value is reached.
Number of receiving computers that are required to begin session before wait time has expired	The number of Symantec Management Agents (excluding the master) that must join a session to enable multicasting to begin. The default value is 100. This setting cannot be less than the value that you specified for Minimum receiving computers per session. This setting can be used to override the wait time when enough agents have joined the session to represent significant bandwidth savings. The wait time is specified in the Wait time to begin session field.
Maximum bandwidth to use for multicasting	The maximum bandwidth that multicasting can use per package. The default value is 125 Kbytes/sec.
Maximum transmission attempts per package	The maximum number of times that the Symantec Management Agent may attempt to receive the same package through multicast. If all attempts fail, the agent reverts to the normal package download procedure. The default number is 3.

Table 3-10 Multicast Configuration settings *(continued)*

Setting	Description
Maximum sessions per physical subnet	Specifies the maximum number of multicast sessions that can occur concurrently per physical subnet. The default number is 10.
Disable multicast for packages smaller than	Specifies the minimum package size that may be downloaded using multicast. The default size is 512 KB.

Targeted Agent Settings: Blockouts tab

The targeted agent blockout periods are times when all communication between the Symantec Management Agent and Notification Server is disabled. The **Blockouts** tab lets you set up any number of blockout periods in a targeted agent settings policy.

See "Configuring the targeted agent settings on Mac computers" on page 61.

Table 3-11 Settings on the **Blockouts** tab

Setting	Description
Disable communication at startup and after blockouts for up to	Disables the communication between Notification Server and the Symantec Management Agents for a specified period. This disabling occurs after the computer is turned on and after a blockout period has expired. This setting prevents all Symantec Management Agents communicating with Notification Server at the same time. For example, at the start of the working day when all the computers are turned on, or after blockouts have finished. The actual time that communication is disabled is a random interval from 0 to the time specified.

Table 3-11 Settings on the **Blockouts** tab *(continued)*

Setting	Description
Time zone	The available time zones are as follows: ■ Use agent time The times are specified without time zone information, and are applied at the local time at each managed computer. Blockouts start and end at different times depending on the time zones of the managed computers. ■ Use server time The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The blockout periods start simultaneously irrespective of time zones, and are compensated for daylight saving. ■ Coordinate using UTC The times are specified with time zone information, where the time zone offset is 0. The blockout periods start simultaneously irrespective of time zones. Daylight savings time does not affect blockout periods.
Blockout periods	The blockout periods that you want to have available. See "Adding a blockout period to the targeted agent settings" on page 71.

Adding a blockout period to the targeted agent settings

You need to specify the blockout periods that you want to use. You can specify any number of blockout periods.

See "Configuring the targeted agent settings on Mac computers" on page 61.

If a blockout prevents a software delivery package download, the package download starts immediately when the blockout expires, according to the download options you selected.

To add a blockout period

1. In the **Blockouts** tab, click **Add Blockout Period**.
2. Specify the Start Time and Duration in the corresponding boxes.

3 In the **Unit** drop-down list, select the blockout period type:

Download	The package server and Symantec Management Agent do not download any software delivery packages. However, the Symantec Management Agent still sends events and gets Symantec Management Agent Settings policy requests from Notification Server. Events and Symantec Management Agent Settings policy requests are typically small amounts of information and have minimal effect on the network traffic. However, packages can be large and can affect the network load. This setting can help minimize the effect of package servers and Symantec Management Agents on the network during business hours.
Total	No communication occurs between the agent on the package server and Notification Server during the specified time period. All events from Symantec Management Agent are queued on the agent and are sent after the blockout.

4 Click **Save Changes**.

Targeted Agent Settings: User Control tab

The targeted agent user control settings are the options that affect what the user of the managed computer can see.

See "Configuring the targeted agent settings on Mac computers" on page 61.

The Mac UI differs from the Windows UI. Although you see the **User Control** tab, the settings you see in Windows do not apply to Mac.

Targeted Agent Settings: Advanced tab

The **Advanced** tab lets you specify an alternate URL that the Symantec Management Agent can use to access Notification Server and turn on the power management feature.

See "Configuring the targeted agent settings on Mac computers" on page 61.

Table 3-12 Settings on the **Advanced** tab

Setting	Description
Specify an alternate URL for the Symantec Management Agent to use to access the NS	Specifies an alternate URL that the Symantec Management Agent can use to access Notification Server. You may need to change these settings when you configure Notification Server to use SSL.
Server Name	We recommend that you use the fully qualified domain name.
Server Web	The Server Web address should be in the following format: **http://<NS_FQDN>:<port>/Altiris/** **https://<NS_FQDN>:<port>/Altiris/**
Enable tickle on Symantec Management Agents	Turns on the power management feature. The relevant settings are specified in the global agent settings policy.

About maintenance windows for managed computers

A maintenance window is a scheduled time and duration when maintenance operations can be performed on a managed computer. A maintenance operation is one that has an effect like the following:

- Changes the state of a computer.
- Causes the computer to restart.
- Interferes with a user's ability to operate the computer.

Maintenance operations include installing software, installing operating system patches, or running a virus scan.

A maintenance window policy defines one or more maintenance windows and is applied to a resource target in the same way as any other policy. These policies provide the maximum flexibility for assigning maintenance windows to computers, without complicating the management of agent settings. If multiple maintenance window policies apply to a single computer, changes to the computer are permitted during any of the maintenance windows.

See "About configuring the Symantec Management Agent for Mac" on page 55.

Using maintenance windows lets you schedule maintenance work on managed computers with minimal effect on workflow and productivity. Also, you can schedule maintenance work on critical servers at different times so no two servers are ever restarted at the same time. You can schedule a maintenance window for

certain times such as daily, weekly, or monthly. The maintenance window can be available indefinitely or restricted to a particular date range.

When you apply a maintenance window to a managed computer, maintenance tasks can only be carried out on them in the scheduled time period. Maintenance tasks include actions such as patches and software deliveries. Symantec Management Agents can download software delivery packages any time, but associated programs can be run only during the maintenance windows.

The Symantec Management Agent processes the policy and provides the functionality that solutions use to determine whether a maintenance window is currently open. Functionality is also provided to allow solutions to inform Notification Server that a maintenance task has been performed.

Many tasks can be combined into a single job. At times it may take longer to complete all tasks in a job than a maintenance window allows for. If the agent has already initiated a task when a maintenance window expires, the maintenance window is automatically extended until the entire job is completed.

See "Configuring maintenance window policies" on page 74.

Configuring maintenance window policies

You can create and modify the maintenance window policies that you need and apply them to the appropriate targets. The default maintenance window policy is applied to all managed computers.

See "About maintenance windows for managed computers" on page 73.

To configure maintenance window policies

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Maintenance Windows**.
2. In the left pane, in the **Maintenance Windows** folder, do one of the following:
   - To create a new maintenance window policy, right-click and then click **New > Maintenance Window**. In the right pane, edit the default new policy name and description as appropriate.
   - To modify an existing maintenance window policy, select the appropriate policy.

3 In the right pane, in the Time Zone box, select the appropriate option:

Use agent time	The times are specified without time zone information and are applied at the local time at each managed computer. Maintenance windows open and close at different times depending on the time zones of the managed computers.
Use server time	The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The maintenance windows open simultaneously irrespective of time zones and are compensated for daylight saving. This option ensures that maintenance windows are always coordinated with the specified local time on the server where the policy is created.
Coordinate using UTC	The times are specified with time zone information, where the time zone offset is 0. The maintenance windows open simultaneously irrespective of time zones. Daylight savings time does not affect maintenance windows.

The time zone applies to all of the maintenance windows that are specified in this policy.

4 If you want the policy to take effect on a particular date, rather than as soon as it is enabled, you can set a start date. In the upper right corner, click **Advanced** and in the **Advanced Options** dialog box, set the start date and end date. Click **OK**.

Start	The date that the policy takes effect. The policy must be enabled in the same way as any other policy. You can enable the policy at any time before or after the start date.
End	If you want the policy to be available for a limited period of time, set the appropriate end date. The policy is unavailable after this date, whether or not it is enabled. This setting is optional. If no end date is specified, the policy is available indefinitely.

5 Create the maintenance windows that you want to include in the policy.

To add a new maintenance window	Click **Add Maintenance Window**.
To delete a maintenance window	Click anywhere in the maintenance window that you want to delete, and then click **Delete**.

6 In each maintenance window, under **Daily Times**, specify the start time of the maintenance window. You must also specify either the end time or the duration in the corresponding boxes.

Alternatively, you can drag the green (start time) and red (end time) arrows to the appropriate places on the time line.

7 Under **Repeat Schedule**, in the Repeat every box, select a schedule and then specify the appropriate schedule filters:

No repeat	The maintenance window is open only once, on the day that it is applied to the managed computer.
Day	The maintenance window is open every day.
Week	Specify the weekdays on which the maintenance window is open.
Month (week view)	Specify the days of the week and the weeks of the month on which the maintenance window is open.
Month (date view)	Specify the dates of the month on which the maintenance window is open.
Yearly (week view)	Specify the days of the week, the weeks of the month, and the months on which the maintenance window is open.
Year (date view)	Specify the dates of the month and the months on which the maintenance window is open.

8 In the **Applied to** panel, specify the maintenance window policy target.

You can select an existing organizational group, filter, or resource target. You can also select individual resources.

Details of the selected items are displayed in the grid. You can view the list by targets, resources, computers, or users, and make any necessary additions and deletions.

9 Click **Save Changes**.

Chapter 4

Discovering Mac computers on the network

This chapter includes the following topics:

- About discovering Mac computers
- Discovering Mac computers
- Creating Network Discovery tasks using the wizard
- Manually creating and modifying Network Discovery tasks

About discovering Mac computers

Network Discovery is basically the same for all platforms. The exception with Mac computers is that to discover them as computer resources, you must enable SNMP before running Network Discovery.

For information about how to enable SNMP on Mac OS X Server, see the Apple support site.

See "Discovering Mac computers" on page 77.

Discovering Mac computers

You can discover all the devices on your network and enter those devices in the CMDB. This process guides you through the steps to discover network devices.

See "About discovering Mac computers" on page 77.

Table 4-1 Process for discovering Mac devices

Step	Action	Description
Step 1	(Optional but recommended) Enable SNMP and configure Network Discovery options.	If you run Network Discovery without enabling SNMP, Mac computers are discovered as generic network devices. To discover Mac computers as network resources, you must enable SNMP before you run Network Discovery. For information about how to enable SNMP on Mac OS X Server, see the Apple support site. You can also configure default task options and SNMP classifications.
Step 2	Create a Network Discovery task.	You can create and schedule a task to discover either a single device or multiple devices on a network. You can use two methods for creating tasks: using the Network Discovery wizard or creating tasks manually. See "Creating Network Discovery tasks using the wizard" on page 79. See "Manually creating and modifying Network Discovery tasks" on page 80.
Step 3	(Optional) Modify task settings or schedules.	After you create a Network Discovery task, you can modify the task settings or add additional schedules. See "Manually creating and modifying Network Discovery tasks" on page 80.
Step 4	View discovery data.	You can view the status of Network Discovery tasks and view reports that show discovery results. Press **F5** to refresh the page and view the status.

Table 4-1 Process for discovering Mac devices *(continued)*

Step	Action	Description
Step 5	Classify unknown devices.	If you have devices with an unknown classification, you can modify the SNMP classifications list. For details, please see Symantec Knowledge Base article TECH155182 titled "Devices are note being identified properly / classified as 'Unknown'."

Creating Network Discovery tasks using the wizard

The Network Discovery wizard is an administrator tool that guides you through creating a discovery task and configuring settings. You can later edit the task's advanced settings and schedules by editing the task.

See "Discovering Mac computers" on page 77.

Ensure that you have enabled SNMP before you begin.

See "About discovering Mac computers" on page 77.

To create Network Discovery tasks using the Network Discovery wizard

1. In Symantec Management Console, on the **Home** menu, click **Discovery and Inventory** > **Network Discovery**.
2. In the **Quick Start Actions**, click **Launch Discovery Wizard**.
3. In the wizard, select a discovery method, and then click **Next**.
4. Specify the portions of the network to discover, and then click **Next**.
5. Select a connection profile, and then click **Next**.

   Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile .
6. Name the task and then click **Next**.
7. Schedule the task, and then click **Finish**.

8 To view the tasks that the discovery wizard creates, view the bottom of the Network Discovery home page.

You may need to click the refresh icon to view newly created tasks. You can also click **Manage** > **Jobs and Tasks** and then in the left pane, click **System Jobs and Tasks** > **Discovery and Inventory**.

Manually creating and modifying Network Discovery tasks

You can manually create and modify tasks from the Task Management Portal. This option lets you configure advanced options and schedules.

See "About discovering Mac computers" on page 77.

See "Discovering Mac computers" on page 77.

When you create tasks manually, you can discover a network or an individual device.

See "To manually create a task to discover a network" on page 80.

See "To manually create a task to discover a single device" on page 81.

To manually create a task to discover a network

1 In the Symantec Management Console, do one of the following:

- In the **Home** menu, click **Discovery and Inventory** > **Network Discovery** and then in Network Discovery Task Management Web part, click **Available Tasks > New**.
- In the **Manage** menu, click **Jobs and Tasks**, right-click **Jobs and Tasks** and select **New > Server Job**, **Client Job**, or **Task**, and from the list in the left pane, under **Discovery and Inventory**, click **Discover Network**.

2 Give the task a unique and a descriptive name.

3 Select a connection profile.

Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile .

4 Select a discovery method.

5 Specify the portions of the network to discover.

6 (Optional) To configure the maximum number of devices to discover concurrently, click **Advanced**.

7 Click **OK** to save the task.

8 In the task window that opens, schedule the task.

9 To view the task, in the left pane, click **Jobs and Tasks** > **System Jobs and Tasks** > **Discovery and Inventory**. You can also view the bottom of the Network Discovery home page. You may need to click the refresh icon to view newly created tasks.

To manually create a task to discover a single device

1 In the Symantec Management Console, in the **Manage** menu, click **Jobs and Tasks**.

2 In the Jobs and Tasks Quick start, click **Create a new job or task**.

3 From the list, under **Discovery and Inventory**, click **Discover Device**.

4 Give the task a unique and a descriptive name.

5 Select a connection profile.

Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile.

6 Click **OK** to save the task.

7 In the task window that opens, click **New Schedule**.

8 Schedule the task.

9 In the schedule dialog, specify the device that you want to discover by entering the IP address or name.

10 Click **Schedule**.

11 To view the task, in the left pane, click **Jobs and Tasks** > **System Jobs and Tasks** > **Discovery and Inventory**. You can also view the bottom of the Network Discovery home page. You may need to click the refresh icon to view newly created tasks.

To modify Network Discovery tasks

1 In the Symantec Management Console, in the **Manage** menu, click **Jobs and Tasks**.

2 To view the default location of Network Discovery tasks, in the left pane, click **Jobs and Tasks** > **System Jobs and Tasks** > **Discovery and Inventory**. You can also view the bottom of the Network Discovery home page.

3 Select a task.

To stop Network Discovery tasks

1. In the Symantec Management Console, in the **Home** menu, click **Discovery and Inventory** > **Network Discovery**.
2. In the Network Discovery Task Management Web part, click **Task Runs**.
3. Select a task and click **Stop**.

Chapter 5

Gathering inventory from Macs

This chapter includes the following topics:

- About using Inventory Solution on Mac computers
- About types of inventory tasks and data for Mac computers
- Installing the Inventory Solution plug-in to the Mac OS X computer
- About Inventory Solution for Mac
- Gathering inventory information about Mac computers using a policy
- Gathering inventory information using a task
- About gathering custom inventory information about Mac computers
- Gathering custom inventory information about Mac computers
- About software inventory using the filescan.rule file on Mac computers
- Using the filescan.rule file to run software inventory on Mac computers
- Scanning for files on Mac computers using a custom file scan rule
- Viewing inventory data of Mac computers in Resource Manager
- Viewing inventory reports for Mac computers
- Troubleshooting Mac problems with Inventory Solution

About using Inventory Solution on Mac computers

Inventory Solution is included in Altiris Client Management Suite 7.1 from Symantec and should already be installed and deployed on your network. When you turn on the policy to install Inventory Solution Plug-in, that policy goes to all computers and all platforms, including Mac computers.

See "About managing the Mac with CMS 7.1" on page 9.

Inventory Solution works on Mac OS X 10.4 and later. Both Power PC and Intel Processors are supported. This topic does not contain information about the functionality of the Inventory for Servers Plug-in, because Inventory Pack for Servers does not support the Mac OS X Server.

If you need help installing or deploying Inventory Solution, please refer to the Inventory Solution user documentation that you installed with CMS 7.1.

Inventory tasks are the same from all platforms, so you follow these familiar steps to gather inventory information from a Mac OS X computer:

- Install Symantec Management Agent to the target computer.
  As usual, you prepare the target Mac for inventory and then deploy the agent. This step is prerequisite to installing the solution plug-in.
  See "Installing Symantec Management Agent to the Mac OS X client computer" on page 33.
- Turn on the Inventory Solution Plug-in policy, which installs the plug-in on the target computer.
  See "Installing the Inventory Solution plug-in to the Mac OS X computer" on page 86.
- (Optional) Create your own Inventory policy or task to gather the information.

Note: You can study the Inventory Solution data model in the following Symantec Connect articles. These articles let you view the information that you can gather from Mac client computers:

- Inventory Solution 7.0 Database Schema - Part 1: Operating System Inventory
- Inventory Solution 7.0 Database Schema - Part 2: Hardware Inventory
- Inventory Solution 7.0 Database Schema - Part 3: Software and User Inventory

About types of inventory tasks and data for Mac computers

You can gather various types of inventory data from the Mac computers in your CMS environment. Inventory data is stored in the data classes that are stored in the Configuration Management Database (CMDB).

See "About Inventory Solution for Mac" on page 87.

After you install Inventory Solution and turn on the Inventory Solution plug-in, you can gather the following categories of inventory information on Mac computers:

- Inventory data. The expanded data that you can gather using Inventory Solution.
  You can gather the following types of inventory information from Mac OS X computers:

Hardware	Processor, storage, physical memory, controllers, peripheral devices, baseboard
Software	Operating system (includes such data as OS name, version, and architecture) and installed software applications (includes such data as file name, size, location, and manufacturer)
Users and groups	Users accounts (includes such information as user name and last login), Admin group members
Files	File name, file type, file size, last modified date, file content (bundle or single file), file permissions, file creation date, product name, product version, product manufacturer

- Custom inventory . The additional data that you can gather beyond the predefined data classes in Inventory Solution.
  You can create the additional data classes that may be unique to your environment. You then run the custom scripts that collect the custom inventory data classes.
  See "About gathering custom inventory information about Mac computers" on page 91.

Please refer to the Symantec Knowledge Base for articles such as the following about Inventory Solution and Macintosh computers:

- HOWTO50111, Custom inventory sample script for UNIX, Linux, and Mac
- HOWTO50109, Customizing the custom inventory sample script for UNIX, Linux, and Mac

- HOWTO36035, Methods for gathering 7.x Inventory Solution output data from UNIX, Linux, and Macintosh clients

Installing the Inventory Solution plug-in to the Mac OS X computer

After you install the Symantec Management Agent on the Mac, you must deploy the Inventory Solution plug-in. This plug-in lets you apply Inventory policies to the client Mac.

This task is a step in the process for preparing a Mac OS X computer for inventory.

After you deploy the plug-in, you can perform advanced Mac administrator tasks such as checking for a successful installation.

See "Checking deployment of the Inventory Solution plug-in to the Mac OS X computer" on page 100.

To deploy the Inventory Solution plug-in to the Mac OS X computer

1. In Symantec Management Console navigate to **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the tree on the left, click **Agents/Plug-ins > Discovery and Inventory > Windows/UNIX/Linux/Mac > Inventory Plug-in Install**.
3. (Optional) Click **Notify user when the task is available** to receive a notification when the Inventory plug-in is delivered to the Mac OS X computer and installed in the Terminal.
4. Turn on the Plug-in installation policy, define scheduling options, and click **Save changes**.
5. On the Mac OS X computer, click **Go > Utilities > Terminal** to open the Terminal.

   You can run this command and all Terminal commands on the physical client computer. Alternately, you can run these commands through an SSH session with the Mac client.
6. In the Terminal on the client Mac or through SSH, enter the following command to force the installation of the plug-in:

   ```
   aex-refreshpolicies
   ```

7 In the Terminal on the client Mac or through SSH, enter the following command to verify that the plug-in has been installed successfully:

```
aex-helper list
```

This command generates a list of installed solutions and subagents. In the Solutions section you see an entry for Inventory.

To view the version of the Inventory plug-in that is installed, enter the following command:

```
aex-inv-helper -v
```

Note that if you receive the message `Command not found`, the plug-in is not installed.

When the plug-in is installed successfully, under **Solutions** you see **Inventory**. Under **Subagents** you see **Altiris Inventory Agent**.

8 In the Terminal on the Mac client or through SSH, enter the following command to check the Inventory plug-in installation log and check the log file for errors:

```
less /opt/altiris/notification/nsagent/aex-inventory-install.log
```

About Inventory Solution for Mac

Symantec Management Platform offers a built-in inventory function that is known as basic inventory.

Inventory Solution lets you gather information beyond the built-in platform inventory. You can gather Mac inventory information using either an inventory policy or an inventory task, the same way you gather Windows inventory information.

You can run a Full inventory to gather all current information. Thereafter, you may want to run a Delta inventory on hardware and software to show what has changed since the previous inventory.

If you want to schedule regular inventory gathering for Mac computers, use a policy.

See "Gathering inventory information about Mac computers using a policy" on page 88.

If you need to force inventory gathering, use the **Run Now** schedule option with the **Gather Inventory** task.

See "Gathering inventory information using a task" on page 90.

Gathering inventory information about Mac computers using a policy

Before you attempt to gather inventory information, ensure that you have installed Symantec Management Agent on the Mac client computer. You must also ensure that the Inventory Solution plug-in is installed and that the plug-in policy is enabled.

See "Installing the Inventory Solution plug-in to the Mac OS X computer" on page 86.

You may also want to enable client logging to facilitate troubleshooting. In the **Advanced options** of the inventory policy, on the **Run options** tab, you check **Enable verbose client logging**. For Mac computers, when you enable this option a separate log file with detailed logging is created for every task. The files are created in the **/opt/altiris/notification/inventory/var/log/** directory.

You can also set a CPU usage priority setting for Inventory: In the **Advanced options** of the inventory policy, on the **Run options** tab, in the **System resource usage** list, select the appropriate CPU usage level.

To gather inventory information using a policy

1 In Symantec Management Console navigate to **Manage > Policies**.

2 In the tree on the left, click **Discovery and Inventory > Inventory**.

You see the following predefined Inventory policies:

Collect Delta Hardware Inventory	The Delta policy sends Full inventory information only the first time. After the Full inventory, the Delta policy only sends hardware inventory changes. Symantec recommends that you enable the Delta policy to reduce network traffic load.
Collect Delta Server Inventory	The Delta policy sends Full inventory information only the first time. After the Full inventory, the Delta policy only sends hardware inventory changes. Symantec recommends that you enable the Delta policy to reduce network traffic load.
Collect Delta Software Inventory	The Delta policy sends Full inventory information only the first time. After the Full inventory, the Delta policy only sends software inventory changes. Symantec recommends that you enable the Delta policy to reduce network traffic load.
Collect Full Inventory	This policy is enabled by default. It runs after you turn on the Inventory Solution plug-in and refresh the policy. When you enable the Full policy, this policy sends all gathered inventory information to Notification Server each time the inventory runs. Symantec recommends that you enable the Delta policy to reduce network traffic load.
Collect Full Server Inventory	When you enable the Full policy, this policy sends all gathered inventory information to Notification Server each time the inventory runs. Symantec recommends that you enable the Delta policy to reduce network traffic load.

3 You can either modify the settings of the predefined policies or create a new policy.

- To modify the settings of the existing policy, click the policy name, change the required settings, and save changes.

- To create a new policy, in the left tree view right-click the **Inventory** folder and from the context menu click **New > Inventory Policy**.

4. Change the required settings of your new policy and click **Save changes**. The inventory-gathering process on Mac computers is nearly identical to the same process on Windows computers or other operating systems. The difference is that you should use appropriate fields for advanced options in the **File properties scan settings** of the policy or task.
5. To force the policy rollout, navigate to **Settings > Notification Server > Resource Membership Update** and under **Complete update schedule** click **Run**.
6. On the Mac OS X computer click **Go > Utilities > Terminal** to open the Terminal.
7. To force the policy to run, enter the following command:

   ```
   aex-refreshpolicies
   ```

8. To verify that the policy is started and running, on the Mac OS X computer enter the following command:

   ```
   aex-cta list --show-all-tasks
   ```

9. After you wait to allow the policy to complete, enter the following command to verify that it succeeded:

   ```
   aex-cta list --show-all-tasks.
   ```

Gathering inventory information using a task

Before you gather inventory information, ensure that you have installed Symantec Management Agent on the Mac client computer. You must also ensure that the Inventory Solution plug-in is installed.

This task is a step in the process for preparing a Mac OS X computer for inventory

To gather standard inventory using an inventory task

1. In Symantec Management Console navigate to **Manage > Jobs and Tasks**.
2. In the tree on the left, right-click **Jobs and Tasks** and click **New > Task**.
3. In the **Create New Task** window, click **Advanced** to select the required task options, and click **OK**.
4. Click **Quick Run** and select your Mac OS X computer.
5. Click **Run** to run the task immediately.

6 On the Mac OS X computer, click **Go > Utilities > Terminal**.

7 To verify that the task has started and is running, enter the following command:

```
aex-cta list --show-all-tasks
```

About gathering custom inventory information about Mac computers

Custom inventory helps you extend the type of inventory you gather by adding the new data classes that are not included by default.

See "About types of inventory tasks and data for Mac computers" on page 85.

Custom inventory also lets you extend the use of a predefined data class by customizing it. For example, the attributes of the Processor Extension data class are Device ID, L2 Cache Size, and L2 Cache Speed. You can customize this data class by adding or removing attributes. If a custom data class is saved in the Configuration Management Database (CMDB) and is empty, you can modify it in the following ways:

- Add nullable, non-nullable, key, and non-key attributes to it.
- Delete its attributes.
- Change the properties of its attributes.

If the custom data class contains data, you cannot modify it. After you customize a data class, you create a task with scripting logic and schedule it to run on the target computers.

Caution: Use caution if you gather inventory using the custom data class and the same data class is also part of the standard inventory. When a standard inventory follows a custom inventory, the data that the standard inventory gathers overwrites the data that the custom inventory gathers.

To prevent the custom inventory data from being overwritten, you must perform the custom inventory after you perform the standard inventory.

See "Gathering custom inventory information about Mac computers" on page 92.

Gathering custom inventory information about Mac computers

See "About gathering custom inventory information about Mac computers" on page 91.

Gathering custom inventory information requires that you complete the following tasks in Symantec Management Console:

- Create and customize a data class.
  Create a custom data class from the data class manager user interface. After you create a custom data class, you can add, edit, and delete its attributes.
  See "To create and customize a data class" on page 92.
- Create a task with scripting logic and schedule it to run on the target computers.
  After you have created the custom inventory data class, you create a custom inventory script task that gathers the custom inventory. The script task is configured with the script to gather the custom inventory and with the schedule of the task.
  You can create a new task or clone an existing sample task and modify it with the custom data classes that you created. To gather the inventory you want, you can use the script that is included in the sample task or you can create your own logic. You can also create an inventory script task on the **Jobs and Tasks** portal page.
  See "To create a custom inventory script task" on page 94.

To create and customize a data class

1. In Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
3. On the **Manage Custom Data Classes** page, click **New data class**.
4. Enter a unique name and a description for the data class and click **OK**.
5. To customize a data class, on the **Manage Custom Data Classes** page, in the data classes list, click the data class.

6 (Optional) To add an attribute to the data class, click **Add attribute** and in the **DataClassAttribute** dialog box, specify the details of the attribute.

To add an attribute that uniquely defines a row in the data class, in the **Key** drop-down list click **Yes**. You enforce that the attribute always has a unique value that is other than NULL.

If the attribute should never be empty or blank, in the **Data required** drop-down list click **Yes**. After you take this action, the **Data required** option is automatically set to **Yes**. You cannot change it unless you click **No** in the **Key** drop-down list.

7 Click **OK**.

8 (Optional) To edit or delete an attribute, select the attribute, and then click **Edit** or **Delete**.

9 (Optional) To let the data class store inventory of multiple objects, check **Allow multiple rows from a single computer resource**.

The data class can store the inventory of services, user accounts, files, network cards, and other objects. When you report inventory values for the columns in a Notification Server Event (NSE), the attributes are identified by the column ID. The attributes are not identified by the column name. As a result, the order of attributes in a data class must be correct. On the **Manage Custom Data Classes** page, you can also specify the sequence of the attributes.

10 Click **Save changes**.

Warning: The final step of saving changes is very important. When you create any data class or add any attributes, all the information is stored in memory. Nothing is created in the database, and on the details page no GUID is assigned until you save changes. As a result, a 00000000-0000-0000-0000-000000000000 GUID is displayed in the property of the data class.

After you click **Save changes** on the **Manage Custom Data Classes** page, the data class is saved in the database, and the GUID is generated.

Note that the GUID changes every time you make changes to the definition of the data class and save it.

To create a custom inventory script task

1. In Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.
3. Right-click the sample custom inventory script task and click **Clone**.
4. In the **Clone** dialog box, give the cloned script a descriptive name and click **OK**.
5. (Optional) Customize the sample script and click **Save changes**.

   To customize the custom inventory sample script for Mac do the following:

Clone or open an existing sample of the custom inventory script task.	Note that the first lines of the script should not be changed. Changes should be made after the `# SCRIPT_BEGINS_HERE` label.
Specify the data class.	Example: `echo UNIX_PS_List`
Specify the delimiters.	Example: `echo "Delimiters=\" \" "`
Specify the data type and the length of each column.	Example: `echo string20 string20 string20 string256`
Specify the column names.	Example: `echo PID Terminal Time Command` Note that the column names are not used in 7.x custom inventory. The column names are left for backward compatibility with 6.x Inventory Solution. You can leave this line empty in 7.x.
Specify commands to retrieve data from system.	Example: `ps -e`
Click **Save changes**.	

6. Under **Task Status**, schedule the task to run on client computers.

About software inventory using the filescan.rule file on Mac computers

A default `filescan.rule` file is included in the Inventory plug-in installation package for each platform. It contains an example list of some common applications. Symantec recommends that you customize the default `filescan.rule`

file to include the additional applications that the software inventory should report.

See "Using the filescan.rule file to run software inventory on Mac computers" on page 96.

A file scan agent that is included in software inventory uses the `filescan.rule` file to detect the applications that are installed on your client computers. The `filescan.rule` file contains the data sets that represent information regarding different applications. The file scan agent compares each data set to the actual file system data to find out whether an application is installed.

Each data set in the `filescan.rule` file consists of two lines of data. The first line is the application description data, and the second line is the matching criteria data. The application description data consists of the product name, the manufacturer, the version, and the description of the application. The matching criteria data includes a file name or the absolute path to the file that is part of the application. The data also includes file size and cyclic redundancy check (CRC).When the file scan agent finds this file in the specified directories, the associated product is reported as a part of that system's inventory.

A data set that represents information about an application in the `filescan.rule` file looks as follows:

```
product name = "Watcher" manufacturer = "Company" version = "3.24"
description = "" file = "/opt/secret/eys/watcher" size = "45698" CRC
= ""
```

You can customize the `filescan.rule` file and add entries for the applications that are developed in-house. After you customize the `filescan.rule` file, you can create a **Quick Delivery** task to redistribute it to all Mac clients.

See "Scanning for files on Mac computers using a custom file scan rule" on page 96.

By default, all local drives and all folders including /Volumes, /Applications, and /Users on those drives are scanned. When you select a folder, all subfolders are included by default. You can add, edit, or delete items in the list. When you use the `filescan.rule` file, if you select only the **File properties** option, the inventory data that is gathered on the client side includes certain properties. These properties include such values as file name, file size, path, and total size of files according to the file scanning rules.

Using the filescan.rule file to run software inventory on Mac computers

Use the `filescan.rule` file to run software inventory so that you can collect information about the installed applications on your Mac computers.

See "About software inventory using the filescan.rule file on Mac computers" on page 94.

To run software inventory using the `filescan.rule` file

1. (Optional) Copy the default filescan.rule file from the client computer to the Notification Server computer and customize it. If you do not need to distribute the file widely, you can edit the file on the client Mac using the `vi /opt/altiris/notification/inventory/etc/filescan.rule` command.
2. (Optional) To distribute the customized `filescan.rule` file to the client computers, in Symantec Management Console create a **Quick Delivery** task.

   Copy the `filescan.rule` file to the following folder:

   `/opt/altiris/notification/inventory/etc/`

   You can use the following universal path with custom installation directories:

   `` `aex-helper info path -s INVENTORY`/etc/ ``
3. For the Inventory policy that gathers software inventory, check the **File properties - manufacturer, version, size, internal name, etc.** option.

Scanning for files on Mac computers using a custom file scan rule

If you want to scan separate folders for files on a local drive using file scan functionality, you create a custom file scanning rule.

See "About software inventory using the filescan.rule file on Mac computers" on page 94.

To create a custom file scan rule

1. In Symantec Management Console, click **Manage > Policies**.
2. Create a new inventory policy and click the **File properties** checkbox.
3. Click **Advanced options** and navigate to **File properties scan settings > Folders**.

4 In the **Mac folders** section, remove all default folders and include the target folder.

5 Click **Scan sub-folders** to scan all subfolders in a parent folder.

6 On the **Files** tab, remove all predefined rules if they are not required and include a new one according to your requirements.

Viewing inventory data of Mac computers in Resource Manager

Inventory information is updated each time Inventory runs. The information that is updated depends on whether you run a Full inventory or a Delta inventory. If you run a Full inventory, all fields are updated. If you run a Delta inventory, only the information that has changed since the previous inventory is updated.

See "About software inventory using the filescan.rule file on Mac computers" on page 94.

To view inventory data in Resource Manager

1 In Symantec Management Console, on the **Manage** menu, click **Filters**.

2 In the left pane, click **Computer Filters > All Computers**.

3 In the right pane, under **Filter Membership**, right-click a computer, and then click **Resource Manager**.

4 On the **Resource Manager** page, perform one of the following actions:

- To view the hardware summary , click **Summaries > Hardware Summary**.
- To view the software summary, click **Summaries > Software Summary**.
- To view the **Installed Software Report**, in the left pane, click **More actions**, and then click **Actions > Installed Software Report**.
- To view the inventory data classes, click **View > Inventory**. To view the data, select a data class. To see the status of the inventory data, click the **Status** tab.
- To view the gathered custom inventory data you need on the created custom data class, click **View > Inventory**. To view the data, select a data class. To see the status of the inventory data, click the **Status** tab.

Viewing inventory reports for Mac computers

In Symantec Management Console you view inventory reports of the information that is gathered from Mac OS X. You can also run reports and export the results.

See "About software inventory using the filescan.rule file on Mac computers" on page 94.

To view inventory reports

1. In Symantec Management Console, click **Reports > All Reports**.
2. Navigate to **Discovery and Inventory > Inventory > Cross-platform** and **Discovery and Inventory > Inventory > UNIX/Linux/Mac** and select the reports that you want to view.

Troubleshooting Mac problems with Inventory Solution

You should enable devnote logging to facilitate troubleshooting.

See "About using Inventory Solution on Mac computers" on page 84.

See "Enabling devnote logging on Mac computers" on page 99.

The following notifications and commands may be helpful when you troubleshoot Mac computers and Inventory Solution:

Verification successful installation of the plug-in: Notification pop-up banner.	The notification banner appears on the client side only if you checked the "Notify user when task is available" box before the plug-in rollout.
The `aex-swdapm` command	The Software Delivery Advertised Package Manager lets you check if the task from the Symantec Management Console is available and execute it manually.
The `aex-helper list` command	The list of objects in the agent registry lets you check if the plug-in installation succeeded.
`less /opt/altiris/notification/ nsagent/aex-inventory-install.log`	This command lets you view the installation log of the plug-in.
Inventory plug-in directories under **/opt/altiris/notification/inventory/...**	The directory contents are as follows: ■ ./etc/ contains config files ■ ./bin/ contains binary files. ■ ./ libraries contains libraries. ■ ./var/ logs contains scripts and libraries.

You may need to take the following actions to resolve common problems:

- Install the Inventory plug-in on clients.
  See "Installing the Inventory Solution plug-in on Mac client computers" on page 102.
- Ensure that the Mac receives the Inventory policy.
  See "Ensuring that the Mac can receive the Inventory policy" on page 99.

You can also refer to the Symantec Knowledge Base for articles about troubleshooting Inventory Solution on Macintosh computers.

Enabling devnote logging on Mac computers

To facilitate troubleshooting, you should enable devnote logging so you have adequate log files to study.

See "Troubleshooting Mac problems with Inventory Solution" on page 98.

To enable devnote logging

1. In the Terminal on the Mac client computer or through SSH, set **Devnote logging level** and **Log size on agent** by entering the `sudo aex-helper agent -s Configuration debug_level devnote` command.
2. Set **Log file size** by entering the `sudo aex-helper agent -s Configuration debug_file_size 0` command.
3. Set the **Backup directory for event saving** by entering the `sudo aex-helper agent -s "Event_queue" backup_dir /path_to_dir/` command.

Ensuring that the Mac can receive the Inventory policy

If the managed Mac does not receive Inventory policy, you can work around the problem.

See "Troubleshooting Mac problems with Inventory Solution" on page 98.

To ensure that the Mac can receive the Inventory policy

1. Make sure that the client is available in the resource target.
2. Perform a client policy refresh using the `aex-refreshpolicy` command.

   Verify /opt/altiris/notification/nsagent/var/policies for the fresh policy file using the `ls -latr` command and then the `aex-cta list` command.
3. Check your scheduling of the policy.
4. Try to update the resource membership for forcing.

Checking deployment of the Inventory Solution plug-in to the Mac OS X computer

After you install the Symantec Management Agent on the Mac and the Inventory Solution plug-in, you can perform advanced tasks. Perform these tasks and all other Terminal commands on the physical Mac client computer or through an SSH session with the Mac client computer.

You can perform these tasks as soon as you have deployed the Inventory Solution plug-in to the Mac OS X computer.

See "Installing the Inventory Solution plug-in to the Mac OS X computer" on page 86.

To check deployment of the Inventory Solution plug-in to the Mac OS X computer

1. On the Mac OS X computer, click **Go > Utilities > Terminal** to open the Terminal.

   You can run this command and all remaining Terminal commands on the physical client computer. Alternately, you can run these commands through an SSH session with the Mac client.

2. (Optional) Click **Notify user when the task is available** to receive a notification when the Inventory plug-in is delivered to the Mac OS X computer and installed in the Terminal.

3. In the Terminal on the client Mac or through SSH, enter the following command to force the installation of the plug-in:

   ```
   aex-refreshpolicies
   ```

4 In the Terminal on the client Mac or through SSH, enter the following command to verify that the plug-in has been installed successfully:

```
aex-helper list
```

This command generates a list of installed solutions and subagents. In the Solutions section you see an entry for Inventory.

To view the version of the Inventory plug-in that is installed, enter the following command:

```
aex-inv-helper -v
```

Note that if you receive the message `Command not found`, the plug-in is not installed.

When the plug-in is installed successfully, under **Solutions** you see **Inventory**. Under **Subagents** you see **Altiris Inventory Agent**.

5 In the Terminal on the client Mac or through SSH, enter the following command:

```
less /opt/altiris/notification/nsagent/aex-inventory-install.log
```

This command lets you check the Inventory plug-in installation log and check the log file for errors.

Checking the inventory information that is gathered with a policy

After you gather inventory information using a policy, you can perform advanced tasks to verify or troubleshoot.

See "Gathering inventory information about Mac computers using a policy" on page 88.

To check the inventory information that is gathered with a policy

1 After you save the changes to your inventory policy, you can force the policy rollout. Navigate to **Settings > Notification Server > Resource Membership Update** and under **Complete update schedule** click **Run**.

2 On the Mac OS X computer click **Go > Utilities > Terminal** to open the Terminal.

3 To force the policy to run, enter the following command:

```
aex-refreshpolicies
```

4 To verify that the policy is started and running, on the Mac OS X computer enter the following command:

```
aex-cta list --show-all-tasks
```

5 After you wait to allow the policy to complete, enter the following command to verify that it succeeded:

```
aex-cta list --show-all-tasks.
```

Checking the inventory information that is gathered with a task

After you gather inventory information using a task, you can perform advanced tasks to verify or troubleshoot.

See "Gathering inventory information using a task" on page 90.

To check the inventory information that is gathered with a task

1 After you click **Run** to run the task immediately, on the Mac OS X computer click **Go > Utilities > Terminal**.

2 To verify that the task has started and is running, enter the following command:

```
aex-cta list --show-all-tasks
```

Installing the Inventory Solution plug-in on Mac client computers

If you cannot install the Inventory Solution plug-in on clients, you may be able to work around the problem.

See "Troubleshooting Mac problems with Inventory Solution" on page 98.

To install the Inventory plug-in on clients

1 Check network setting and DNS name resolving:

```
/etc/resolv.conf
```

```
/etc/hosts
```

2 Check if Inventory Installation policies are enabled on server side.

3 Make sure that client is available in resource target (using resource membership updating for forcing). In Symantec Management Console click **Settings > Notification Server > Resource Membership Update** and in **Complete update schedule**click **Run** .

4 Perform a refresh policy on client side, using the `aex-refreshpolicy` command.

5 Download inventory packages from the server.

Step 1 In the GUI click **Finder > Go > Connect to server (*Your SMC Server*\NSCap\bin\UNIX\Inventory\Mac\universal)** and install it manually, where *Your SMC Server* is the name of your server.

Step 2 In Symantec Management Console in the root folder create a directory named **share** using the `mkdir share` command. Then, mount the Inventory plug-in folder using the following command:

```
mount_smbfs
//[domain;][user[:password]@]server[/share] share
```

The command looks like the following:

```
mount_smbfs //USER:PASSWORD@SERVER/NScap/bin/
unix/inventory/mac/universal share
```

Step 3 To install the Inventory plug-in manually, complete the following steps:

- From the server, copy **AltirisInventory.pkg.tar.gz** and **rollout.sh** to the client computer.
- Open the folder to which you copied the files, and execute the `sh rollout.sh` command.

Chapter 6

Software Management Solution for Mac

This chapter includes the following topics:

- About delivering Mac software with Software Management Solution
- Components of Software Management Solution specific to Mac computers
- What you can do with Software Management Solution on Mac computers
- Implementing Software Management Solution on Mac computers
- About the agents and plug-ins that Software Management Solution uses
- About Software Management Solution settings for Mac computers
- Schedule settings for Managed Software Delivery to Mac computers
- Download settings in Software Management Solution for Mac computers
- Run settings in Software Management Solution for Mac computers
- Results-based actions settings in Software Management Solution for Mac computers
- Advanced options in Managed Software Delivery policies for Mac computers
- Advanced options for tasks in Software Management Solution for Mac computers
- Methods for delivering software to Mac computers

About delivering Mac software with Software Management Solution

Software Management Solution is included in Altiris Client Management Suite 7.1 from Symantec and should already be installed and deployed on your network. Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It significantly reduces desktop visits and lets you easily support your mobile work force.

Software Management Solution also lets users directly download and install approved software or request other software.

Software Management Solution integrates with the Software Catalog and the Software Library that are part of the Symantec Management Platform. By leveraging this information, Software Management Solution ensures that the correct software gets installed, remains installed, and runs without interference from other software. This integration lets your administrators focus on delivering the correct software instead of redefining the packages, command lines, and so on for each delivery.

For more information, see the topics about the Software Catalog and the Software Library in the *Symantec Management Platform Help*.

When you install Symantec Management Platform and Client Management Suite 7.1, you see enhanced console views. The enhanced Symantec Management Console views replace the default console views through Symantec Management Platform version 7.0 for computers and software. For tasks and policies, the enhanced views add drag-and-drop functionality. In addition, you can now search the tree rather than drilling down to find specific tasks or policies.

The enhanced console views apply to the following options on the Symantec Management Console **Manage** menu:

- **Computers**
- **Software**
- **Software Catalog**
- **Jobs and Tasks**
- **Policies**

Many procedures have been updated to reflect these enhanced views. A getting started guide for users who have installed one of the listed products is available at the Symantec documentation Web site.

IT Management Suite 7.1 from Symantec Enhanced Console Views Getting Started Guide

Software Management Solution supports packages for the Windows, UNIX, Linux, and Mac operating systems. With few exceptions, all the functions in Software Management Solution work the same for all platforms. For example, you use the same method to create a delivery task for a Windows, UNIX, Linux, or Mac OS package.

An important exception is Software detection rules . These rules work only on the Windows platform.

See "Key CMS Mac capabilities and limitations compared to Windows" on page 13.

For a complete list of the platforms that Software Management Solution supports, see the *Software Management Solution Release Notes*.

See "Components of Software Management Solution specific to Mac computers" on page 107.

See "What you can do with Software Management Solution on Mac computers" on page 108.

Components of Software Management Solution specific to Mac computers

The components of Software Management Solution let you deliver and manage software on client computers.

Table 6-1 Components of Software Management Solution

Component	Description
Software delivery tasks and policies	You can use any of several methods to deliver software to client computers. The method that you use to create the task or policy depends on your delivery requirements. See "Methods for delivering software to Mac computers" on page 119.
Software Portal	The Software Portal is a Web-based interface that is installed on the client computers. With the Software Portal, users can request and install software with little or no administrator involvement. See "About the Software Portal" on page 132.

See "What you can do with Software Management Solution on Mac computers" on page 108.

What you can do with Software Management Solution on Mac computers

Software Management Solution lets you distribute and manage the software that is used in your organization.

Table 6-2 What you can do with Software Management Solution

Task	Description
Configure the default settings for Managed Software Delivery policies.	Configuration settings control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies. Then you can change the settings for a specific policy only when needed. See "About Software Management Solution settings for Mac computers" on page 111.
Perform an advanced software delivery.	Managed Software Delivery simplifies your advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources and their dependencies. For example, you can create a single Managed Software Delivery policy that installs an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. See "About advanced software deliveries" on page 121.
Perform a Quick Delivery of a single software resource.	You can perform a Quick Delivery of a single software resource that runs with minimum configuration. You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Because the software resources and the delivery settings are predefined, Quick Delivery makes it easy for administrators and non-administrators to deliver software.
Deliver a package without defining a software resource.	Package Delivery lets you quickly push out any package regardless of whether it is associated with a software resource.
Deliver the tasks and packages that were created in Altiris Software Delivery Solution 6.x.	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.x, you can migrate your software-related tasks and packages. For more information about 6.x data migration, see the *Symantec Management Platform Release Notes*.
Deliver software to fulfill user requests.	By using the Software Portal, users can request and install software through a Web-based interface with little or no administrator involvement. See "About the Software Portal" on page 132.

Implementing Software Management Solution on Mac computers

Before you use Software Management Solution to manage software on Mac computers, you must set it up and prepare it for use.

The prerequisites for implementing Software Management Solution are as follows:

- Symantec Management Platform and Software Management Solution must be installed on the Notification Server computer.
  For details, see the ITMS 7.1 Implementation Guide at http://www.symantec.com/docs/DOC3464.
- The Symantec Management Agent must be installed or upgraded on the computers that you plan to manage.
  Software Management Solution requires that target computers be managed. A managed computer is one on which the Symantec Management Agent is installed.
  For more information, see the topics about installing or upgrading the Symantec Management Agent in the *Symantec Management Platform Help*.
- You must install or upgrade the Symantec Management Agent on the Mac computers that you plan to manage.
  The Software Portal for Mac is installed automatically with the Software Management Plug-in.
  For more information, see the topics about installing or upgrading the Symantec Management Agent for UNIX, Linux, and Mac in the *Symantec Management Platform Help*.

Table 6-3 Process for implementing Software Management Solution

Step	Action	Description
Step 1	Install or upgrade the Software Management Solution plug-in on managed computers. In Symantec Management Console, enable the policy.	The Software Management Solution plug-in is required for you to deliver and manage software on client computers. Perform this step every time that you need to install the Software Management Solution plug-in on the client computers that do not have it. The unified **Software Management Solution Plug-in Install** policy lets you install the solution plug-in on all supported operating systems. You may have performed this step when you installed the Symantec Management Platform or when you added new computers to the network.

Table 6-3 Process for implementing Software Management Solution *(continued)*

Step	Action	Description
Step 2	Configure security privileges for Software Management Solution.	Administrators need the appropriate privileges to deliver and manage the software in your organization. You or another administrator may have already performed this step when you configured security for the Symantec Management Platform. For more information, see the topics about setting up security and Software Management Solution settings in the *Symantec Management Platform Help*.
Step 3	Configure default settings for Managed Software Delivery.	You can configure the settings that control the behavior of Managed Software Delivery policies. Rather than configuring these settings individually for each policy, you can configure the default settings that apply to all new Managed Software Delivery policies.

About the agents and plug-ins that Software Management Solution uses

The information in this topic is specific to Mac computers.

Certain agents and plug-ins must be installed on the client computers to manage and run the Software Management Solution functions.

Predefined tasks are provided to install these agents and plug-ins.

Table 6-4 Agents and plug-ins that Software Management Solution uses

Agent or plug-in	Description
Software Management Framework agent	Manages all the software delivery functions in Software Management Solution. Software deliveries are closely integrated with the software resources in the Software Catalog. The Software Management Framework agent manages the package downloads and other aspects of software delivery. The Software Management Framework agent is installed on the client computers when the Symantec Management Agent is installed. For more information, see the topics about the Software Management Framework agent in the *Symantec Management Platform Help*.

Table 6-4 Agents and plug-ins that Software Management Solution uses *(continued)*

Agent or plug-in	Description
Software Management Solution Plug-ins	In 7.1 one unified console-side Software Management Solution Plug-in supports software delivery and software management on the Mac platform. Although Software Management Solution plug-ins for Mac and other UNIX-based platforms differ from plug-ins for Windows clients, the policies that manage client-side installation, upgrade, and uninstallation are unified on the console side for all platforms. A unified plug-in means that you enable the same installation, upgrade, or uninstallation policy for managing the Software Management plug-in on all clients. You use the same plug-in for Mac clients that you use for Windows clients. The software resources that comprise this plug-in are as follows, in alphabetical order: ■ Software Management Plug-in for AIX ■ Software Management Plug-in for HP UX ■ Software Management Plug-in for Linux ■ Software Management Plug-in for Mac ■ Software Management Plug-in for Solaris

About Software Management Solution settings for Mac computers

Software Management Solution settings control the behavior of the software-related policies and tasks. The default settings let administrators create policies and tasks without having to enter the details that they are not familiar with. Instead, a more experienced administrator can configure the default settings that apply to all the new policies and tasks that are created. When necessary, the administrator who runs the specific policies and tasks can change the settings.

Table 6-5 Sources of default settings for Software Management policies and tasks

Policy or task	Source of default settings
Managed Software Delivery	All new managed software delivery policies inherit the default settings that are defined on the **Managed Delivery Settings** page. You can override the default settings for specific Managed Software Delivery policies. Changing the default settings for managed software delivery does not affect the execution of the managed software delivery policies that were created earlier.
Package Delivery Quick Delivery	Some of the task settings are predefined. Other settings for these tasks are obtained from the Task Management settings.

Schedule settings for Managed Software Delivery to Mac computers

The Schedule settings let you define the schedule on which a Managed Software Delivery policy runs. You schedule the compliance check and the remediation action separately.

Managed Software Delivery policies perform compliance checks and remediations. A compliance check uses the software resource's unique identifier to determine the state of the software on a managed computer. If the software is not in the correct state, the compliance check fails and remediation occurs. The nature of the remediation depends on the action that the Managed Software Delivery policy performs. For example, the remediation can consist of installing or uninstalling the software.

The Schedule settings appear in multiple places in the Symantec Management Console as follows:

On the **Managed Delivery Settings** page	Lets you define the default settings for all new Managed Software Delivery policies. You can override these settings for a specific policy.
On the **Schedule delivery** page that appears during the **Managed Software Delivery** wizard	Lets you change the settings for a specific policy.

Under the **Schedule** section that appears when you create or edit a Managed Software Delivery policy	Lets you change the settings for a specific policy.

For more information, see the topics on specifying a policy schedule in the *Symantec Management Platform Help*.

Table 6-6 Schedule settings for Managed Software Delivery: **Compliance**

Option	Description
Add Schedule	Lets you add one or more schedules to the policy. You can specify as many schedules as you need, and you can have any number of schedules active at one time.
Time zone	Lets you specify the time zone to apply to the schedule.
No repeat	Lets you specify the interval at which to rerun the Managed Software Delivery, if any. This option is available only when you schedule a specific time or a specific window. Use this option to perform recurring compliance checks and remediation actions.
Advanced	Lets you set the options that determine the conditions under which the check is performed and the effective dates for the policy.

Table 6-7 Schedule settings for Managed Software Delivery: **Remediation**

Option	Description
Your point of entry into these settings determines what text appears, as follows: ■ **When computers are found to be out of compliance, run remediation actions** ■ **Choose when to remediate when compliance fails**	Specify when to perform any remediation action that is defined for the Managed Software Delivery. The options are as follows: ■ **Don't run remediation** Lets you run a Managed Software Delivery policy without performing the remediation. For example, you might want to perform an applicability check or a compliance check to determine if a certain configuration exists. A report of the results of the check might be all you need, or you might perform some action other than installing or uninstalling software. ■ **Immediately** ■ **At next maintenance window** Lets you delay the remediation until the next maintenance window. If a maintenance window is not set up for the target computer, remediation is run immediately. For more information about maintenance windows, see *Symantec Management Platform Help*. ■ **Schedule** You can run remediation at a specific time.

Download settings in Software Management Solution for Mac computers

The **Download** settings let you define how the packages and command lines are downloaded for a policy or a task in Software Management Solution.

These settings appear in the following places:

On the **Managed Delivery Settings** page	Lets you define the default settings for all new Managed Software Delivery policies. You can override these settings for a specific policy.
In the **Advanced Options** dialog box that you can access when you edit a Managed Software Delivery policy.	Lets you change the settings for any specific software resource that the policy contains. The changes that you make for a specific policy do not change the defaults for other policies.

In a Software Management Solution task, these settings appear in the **Advanced Options** dialog box, on the **Download Options** tab.	Lets you change the default settings for a specific Software Management Solution task.

Table 6-8 **Download** settings

Option	Description
Destination download location	Lets you define the directory on the client computer in which to place the package file. The package downloads to and runs from this location. Options for the download location are as follows: ■ **Symantec Management Agent cache** Places the package files in the default directory for software packages. The default location of the Symantec Management Agent cache on a Mac computer is as follows: /opt/altiris/notification/nsagent/var/packages/*GUID* ■ **Location on destination computer** Lets you override the default directory and download the package directly to a directory that you specify. This option applies to both UNIX-style directories including Mac computers and to Windows computers.
Use the default Symantec Management Agent download settings to download	Lets you download and run the package with the default Download and Execute settings that are defined in the global Symantec Management Agent settings. These settings determine whether the package runs from the server or on the client computer. The Software Management Solution tasks do not support the multicasting option, even if it is selected in the global Symantec Management Agent settings.
Delete package from client computer	Deletes the packages that are downloaded to the client computer but that are not used for the specified amount of time. The specified amount of time is the amount of time that you select in the **If unused for** drop-down list.

Run settings in Software Management Solution for Mac computers

The **Run** settings let you define how a Managed Software Delivery policy runs on the client computer. They also let you define how much you let the user interact with the policy.

The **Run** settings are arranged in sections. The appearance and location of the sections depend on how you access the settings.

Table 6-9 Sections on the **Run** tab

Section	Description
Results-based actions section	The options in this section let you define the actions that occur during or after the policy runs on the client computer. In a Managed Software Delivery policy, the **Results-based actions** section appears in the **Advanced Options** dialog box, on its own tab.
Reporting section	The option in this section defines the level of detail that is logged when a policy runs on the client computer. In a Managed Software Delivery policy, the **Reporting** section appears on the **Policy settings** tab.

Results-based actions settings in Software Management Solution for Mac computers

These settings let you define the actions that occur during or after the Software Management Solution policy runs on the client computer.

These settings appear in the following places:

On the **Managed Delivery Settings** page, on the **Run** tab.	Lets you define default settings for all new Software Management Solution policies.
In a Managed Software Delivery policy, these settings appear in the **Advanced Options** dialog box, on the **Results-based actions** tab.	Lets you change the settings for a specific software resource that the policy contains. The changes that you make for a software resource in a specific policy override the global settings.

Table 6-10 Options in the **Results-based actions** section or tab

Option	Description
Upon success run	Lets you define an action to occur after the policy runs successfully. The options are as follows: ■ **No action required** ■ **Restart computer** ■ **Log off user**
Terminate after	Lets you define the amount of time to wait before the policy terminates if it stops responding.
Upon failure	Defines whether the policy aborts, continues, or restarts when it fails. When you create a Managed Software Delivery policy, this setting is the same for each software resource and task that the policy contains. You can edit the policy to override this setting for each software resource and task. For example, if the execution of the first software resource fails, you can run subsequent items. Conversely, if one execution in the sequence fails, you can abort the remaining items in the sequence. This option applies to both the applicability check and the execution. If an applicability rule fails for a software resource that is set to abort upon failure, then the policy does not continue. The policy does not continue even if other applicability rules succeeded. Also, any subsequent tasks and software resource deliveries that are in that policy do not continue either. If you want to evaluate all rules, choose the **Continue** option. If you choose **Continue**, compliance status of the policy is not affected with the software.
Max retries	Defines the number of times that the policy retries when it fails.

Advanced options in Managed Software Delivery policies for Mac computers

This dialog box lets you change the settings for the individual software resources that are in a specific Managed Software Delivery policy. For example, you might download this software's package to a different location or allow the user to interact with this software's installation but not others.

These settings are inherited from the policy but you can change them for any and all the software resources in the policy. The changes that you make for a specific policy do not change the defaults for other policies.

The **Advanced options** dialog box appears when you edit a Managed Software Delivery policy, select a specific software resource, and click **Advanced options**.

Table 6-11 Tabs in the **Advanced options** dialog box

Tab	Description
Download tab	Defines how a specific software resource downloads to the client computer.
Results-based actions tab	Defines the actions that occur during or after the policy runs on the client computer.

Advanced options for tasks in Software Management Solution for Mac computers

This dialog box lets you change the settings that define how a specific task runs. These settings are predefined to make task creation easier and to maintain consistency across your organization. However, you can change the default settings for a specific task. For example, you can run the task with different user credentials. The changes that you make for a specific instance of a task do not change the defaults for other instances of that task.

When you create or edit a task in Software Management Solution, the **Advanced** option provides access to the task settings.

Table 6-12 Tabs in the **Advanced settings** dialog box

Tab	Description
Download Options tab	Contains the settings that define how a specific task downloads and runs on the client computer. The defaults for some of these settings are inherited from the Symantec Management Agent settings.
Run options tab	Contains the settings that define how a specific software management task runs on the client computer. The defaults for these settings are inherited from the Task Server settings.

The tasks that use these settings are as follows:

- Package Delivery
- Quick Delivery

Methods for delivering software to Mac computers

You can deliver software to one or more managed computers by creating and running a Software Management task or policy. The method that you use to create the task or policy depends on your delivery requirements.

Table 6-13 Methods for delivering software

Your requirement	Delivery method	Description
Deliver software to a specific computer or to a group of computers.	Drag and drop	In Symantec Management Console under **Manage > Software**, you can click and drag Deliverable software to a target. The target can be a single computer or a group of computers that you have already defined under **Manage > Computers** In the **Manage > Software** window, the **Installed Software** subpane lists the deliverable software packages that are on the server, including software releases and software updates. Deliverable software is the software that has a package or command line associated with it. If you drag and drop the package onto a computer, the package or command line installs the software. If software appears in this list, then it is ready to deploy. When you double-click a deliverable software package, the installation details open and you can define or make changes to the installation details.
Perform a Quick Delivery of a single software resource.	Quick Delivery	You can use the task-based Quick Delivery method to specify the software to deliver, the action to perform, and the computers to deliver to. Quick Delivery uses the default task settings, which you can change when necessary. Because of its simplicity, Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver software safely and accurately. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog.

Table 6-13 Methods for delivering software *(continued)*

Your requirement	Delivery method	Description
Perform one or more of the following advanced delivery actions: ■ Deliver on a recurring schedule. ■ Install software with the other software that it depends on. ■ Install a software resource that replaces other software. ■ Sequentially install multiple software and tasks. ■ Run any client task at any stage of the delivery. A client task is one that is defined in Notification Server and is intended to run on a client computer.	Managed Software Delivery	Managed Software Delivery is a policy-based delivery method that lets you fulfill advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions. The software that you deliver in this way must be defined as a deliverable software resource in the Software Catalog. Managed Software Delivery leverages the software resource information and the logic that is in the Software Catalog. For example, Managed Software Delivery uses the software resource's dependencies, package, and detection rule. See "About advanced software deliveries" on page 121.
Deliver software in response to a direct request from a user.	Software Portal	With the Software Portal, users can request software and responds to those requests. If the user is pre-approved to install the software, the installation occurs without the administrator's involvement. Otherwise, the administrator only needs to approve the requests and deliver the software that is not in the Software Catalog. See "About the Software Portal" on page 132.
Deliver software with a policy that you migrated from Software Delivery Solution 6.x.	Legacy Software Delivery	When you upgrade from Notification Server 6.x to Symantec Management Platform 7.x, you can migrate your 6.x software delivery tasks to Legacy Delivery policies. You can continue to use those policies as they are. You can also assign their packages to software resources to deliver a 6.x software package with Quick Delivery or Managed Software Delivery.

Chapter 7

Managed Software Delivery to Mac computers

This chapter includes the following topics:

- About advanced software deliveries
- Advanced delivery actions that Managed Software Delivery can perform with Mac computers
- About the execution of Managed Software Delivery policies on Mac computers
- About software policy remediation on Mac computers
- Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers
- Select Software dialog box
- Policy Rules/Actions section for Mac computers
- Policy Rules/Actions: Software tab for Mac computers
- Policy Rules/Actions: Policy settings tab for Mac computers
- About the Software Portal

About advanced software deliveries

In many organizations, administrators spend the majority of their software delivery time on a minority of advanced delivery activities. Managed Software Delivery simplifies advanced software deliveries by letting you deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single Managed Software Delivery policy that installs

an application and its associated patches and service packs. Managed Software Delivery can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.

Managed Software Delivery is a policy-based delivery method that lets you respond to an assortment of advanced delivery requirements.

The power of Managed Software Delivery lies in the following abilities:

- To intelligently perform the compliance checks and the remediation actions that let you not only deliver software but also manage it.
- To leverage the software resource information and the logic that is in the Software Catalog such as dependencies, packages, and detection rules.
- To conserve bandwidth by downloading packages only when they are needed. If a client computer does not have the appropriate configuration for the software or if the software is already installed, the package is not downloaded.
- To perform multiple delivery actions with a single policy.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software is not defined, contact an administrator who can edit the Software Catalog.

If you need to perform a Quick Delivery of a single software resource, use Quick Delivery instead of Managed Software Delivery.

Advanced delivery actions that Managed Software Delivery can perform with Mac computers

Managed Software Delivery is a policy-based delivery method that lets you respond to an assortment of advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions.

See "About advanced software deliveries" on page 121.

Table 7-1 Advanced delivery actions that Managed Software Delivery can perform

Delivery action	Description
Deliver software	In its simplest form, Managed Software Delivery delivers a single software resource with its associated package and command line. It downloads the software and installs it on the managed computer according to a defined schedule. It does not perform a compliance check and it always considers the computer to be compliant.

Table 7-1 Advanced delivery actions that Managed Software Delivery can perform *(continued)*

Delivery action	Description
Remediate software on the client computer	Managed Software Delivery installs the software to a specific known state on the client computer. If the state of the software is out of compliance, Managed Software Delivery performs a remediation to restore the correct state.
Deliver software dependencies to the client computer as needed	Managed Software Delivery checks the client computer for the dependencies of a software resource that it delivers. When a client computer does not contain the dependency software, Managed Software Delivery can perform a remediation by installing the missing dependency. You can choose whether to check dependency tasks or not, with the following results: ■ If you do not choose to check dependency tasks, the Managed Software Delivery policy proceeds and either installs or fails. ■ If you choose to check dependency tasks, those tasks are checked and installed if necessary.
Sequentially install multiple software resources and tasks	You can deliver multiple software resources and tasks with a single Managed Software Delivery policy. You can add any client tasks to the execution queue to perform custom operations before, during, or after the software remediation process. For example, you can add a task that performs a restart or runs a script. A client task is one that is defined in Notification Server and is intended to run on a client computer.
Execute software installations offline	In a Managed Software Delivery policy, you can set different schedules for the compliance check and the remediation (in this case, installation). The separate schedules allow for the offline execution of the Managed Software Delivery. When the compliance check determines that a remediation is required, the policy downloads the appropriate package. Remediation can occur even if the client computer is not connected to the server because the client computer already has the package that it needs.

About the execution of Managed Software Delivery policies on Mac computers

When a Managed Software Delivery policy runs on a managed computer, it performs a series of tasks that are grouped into the following phases:

- Compliance
  See Table 7-2.
- Remediation
  See Table 7-3.

When you schedule a Managed Software Delivery policy, you can assign different schedules for compliance and remediation. For example, you can schedule the compliance status to be reported during the day and the remediation to occur only during a maintenance window.

The ability to separate compliance and remediation also allows for the offline execution of Managed Software Delivery policies. When the compliance check determines that a remediation is required, the policy downloads the appropriate package. Remediation can occur even if the client computer is not connected to the server because the client computer already has the package that it needs.

Table 7-2 How the compliance phase of Managed Software Delivery works

Step	Action	Description
Step 1	Policy execution	Starts the policy's compliance process at the scheduled time on the client computer.
Step 2	Compliance check	Evaluates the software resource's unique identifier to determine whether the software resource is installed on the client computer. The software resource's unique identifier is used when the software resource is not associated with a detection rule. Because detection rules for Mac computers are not implemented in Software Management Solution in 7.1, the SMF cache must be checked to determine if software is installed. The compliance check checks the cache (swc.dat file) This is how the detection rule works with Mac computers. If all the software in the Managed Software Delivery policy is in the correct state, it is compliant. Therefore, remediation is not needed and the policy execution stops. If any or all of the software is not in the correct state, it is out of compliance. Therefore, remediation is required and the policy execution continues.

Table 7-2 How the compliance phase of Managed Software Delivery works *(continued)*

Step	Action	Description
Step 3	Package download	Downloads the package for each software resource or task in the Managed Software Delivery policy that requires a package. The package download might not be required when the remediation action is to uninstall the software. In that case, the package download is skipped. The Managed Software Delivery policy downloads the package as follows: ■ Download the package to the client computer. ■ Create a snapshot of the package that is on the client computer and compare it to the snapshot on the package server. If the package is already on the client computer because of a recurring delivery or a delivery re-attempt, its existing snapshot is used for comparison. ■ If the snapshots do not match, re-download the package. A mismatch can occur when some kind of interception has corrupted the package. When the package download is successful, the compliance process is finished and the policy is ready for the remediation process.

Table 7-3 How the remediation phase of Managed Software Delivery works

Step	Action	Description
Step 1	Compliance check	Determines whether the software is installed on the client computer. Because no detection rules for Mac computers are implemented in Software Management Solution in 7.1, you should check the SMF cache. Check the cache (swc.dat file) to determine if software is installed. This compliance check ensures that the software is still in the same state as it was during the compliance process. For example, if the remediation was scheduled to run later than the compliance process, the software might have been installed or uninstalled in the interim. If the remediation is still required, the process continues.
Step 2	Remediation action	Installs, uninstalls, or performs any other remediation action that the software requires. If the Managed Software Delivery policy contains multiple software resources and tasks, they are executed in the order in which they appear in the policy. You can override the policy's remediation settings and schedule for individual software resources and tasks within the policy.

Table 7-3 How the remediation phase of Managed Software Delivery works *(continued)*

Step	Action	Description
Step 3	Report to Notification Server	The Symantec Management Agent on the client computer reports the results of the Managed Software Delivery process to Notification Server. You can obtain information about the results from the compliance reports and the delivery reports in Software Management Solution.

See "About advanced software deliveries" on page 121.

About software policy remediation on Mac computers

Managed Software Delivery lets you not only deliver software but also manage it. These actions ensure that you deliver the correct software to the correct computers.

When you schedule a Managed Software Delivery policy, you can assign different schedules for compliance and remediation. For example, you can schedule the compliance process to occur during the day and the remediation to occur only during a maintenance window.

Table 7-4 Compliance and remediation actions

Action	Description
Compliance	Compliance on Mac computers depends on the delivery method you select to install the software, as follows:Using Quick Delivery or Managed Delivery installs the software. ■ If you select Quick Delivery to install the software, then no detection is executed. In this case, you execute a command line command. To determine which software is installed on a Mac client computer, you must create a Software Inventory task that runs periodically and detects installed software. As a result of running this task, the information appears in Notification Server. ■ If you select Managed Software Delivery, when you execute delivery you first verify in your local cache if the software was installed previously. This cache is located inside the `swc.dat` file in the SMFagent on the client side. If a record of the software is present in that file, then delivery is not executed. If no information about the software is in the cache, then you execute a command line. You have the following options for ensuring that software appears in the cache: ■ If you installed the software manually, when you set Software Inventory to run the cache is also updated. ■ If software is installed using Managed Software Delivery, the cache is updated when the software delivery is executed.

Table 7-4 Compliance and remediation actions *(continued)*

Action	Description
Remediation	Remediation is the act of fixing any software that is out of compliance on the client computer. The nature of the remediation depends on the command-line action that the Managed Software Delivery policy performs. For example, an installation command runs when the compliance check returns False, and an uninstall command runs when the compliance check returns True. The following example illustrates how the installation command line determines the remediation action: Assume that you want to install antivirus software on all managed computers that do not have it installed. You create the Managed Software Delivery policy and select an installation command line. When the policy runs, the compliance check determines whether the specified antivirus software is installed.

Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers

You can perform one or more advanced software delivery actions with a single Managed Software Delivery policy. Creating a Managed Software Delivery policy is the first step in performing an advanced software delivery.

See "About advanced software deliveries" on page 121.

The **Managed Software Delivery** wizard provides a quick way to create and schedule a policy for a single software resource and its dependency software. We recommend that you use the wizard because it can include any dependency software and warn you of software associations.

When you create a Managed Software Delivery policy with the **Managed Software Delivery** wizard, the policy is enabled automatically. If you do not want the policy to be available to managed computers immediately, edit the policy, and disable it. You can also edit the policy to add information about what to deliver.

The software that you deliver in this way must be defined as a software resource in the Software Catalog. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

You can run the **Managed Software Delivery** wizard from the **Manage > Software** view or from other areas of the Symantec Management Console. Your point of entry into the **Managed Software Delivery** wizard determines the amount of default information that is populated.

Create the policy without the wizard if you need to do any of the following things:

- Add multiple software resources and tasks.

- Override the default settings.

To create a Managed Software Delivery policy with the Managed Software Delivery wizard

1. In the Symantec Management Console, on the **Manage** menu, click **Software**.
2. In the left pane, under **Deliverable Software**, click **Software Releases**.
3. Right-click a software resource and then click **Actions > Managed Software Delivery**.

   If the **Managed Software Delivery** option is not available, the software resource does not have a package associated with it and cannot be delivered. Click **Actions > Edit Software Resource** and configure the software resource.
4. In the **Managed Software Delivery** wizard, on the **Select software** page, specify the software to deliver and other delivery options and then click **Next**.
5. On the **Select destinations** page, specify the destinations to deliver the software to and then click **Next**.
6. On the **Schedule delivery** page, define the schedule for running the Managed Software Delivery and then click **Next**.
7. (Optional) On the **Specify dependencies and updates** page, select any dependencies, updates, or service packs that are defined for this software resource and then click **Next**.

Dependencies	Check **Verify dependencies** and select the check box for each dependency to include.
Updates or service packs	Select the check box for each update or each service pack to include.

8. To complete the wizard, click **Deliver Software**.

Select Software dialog box

This dialog box lets you select a software resource to act upon. This dialog box can appear in multiple areas of the product that require a software resource to be specified. For example, it appears when you add a software resource to a Managed Software Delivery policy.

See "About advanced software deliveries" on page 121.

Policy Rules/Actions section for Mac computers

This section appears when you create or edit a Managed Software Delivery policy. It lets you add software resources and tasks to the policy and change the settings for the policy.

Table 7-5 Tabs in the **Policy Rules/Actions** section

Tab	Description
Software	Lets you define the software and tasks to deliver and set the options for each software resource and task.
Policy settings	Lets you change the default settings for the Managed Software Delivery policy.
Software Publishing	Lets you publish the Managed Software Delivery policy to the Software Portal.

Policy Rules/Actions: Software tab for Mac computers

This tab lets you define the software to deliver. You can select a single software resource or you can select multiple software resources and tasks to create a sequential delivery policy. This tab also lets you set options for the individual software resources and tasks.

This tab appears when you create or edit a Managed Software Delivery policy.

See "Creating a Managed Software Delivery policy with the Managed Software Delivery wizard for Mac computers" on page 127.

After you select a software resource, this tab contains the following sections:

Left pane
: Displays the sequence of software resources and tasks that this policy delivers. You can add software resources and tasks.

  See Table 7-6.

  When you click a specific software resource or task, its settings appear in the right pane.

Right pane
: Lets you override the policy settings for the specific policy or task. The settings that appear differ depending on whether you click a software resource or a task.

  See Table 7-7.

  See Table 7-8.

Table 7-6 Options for adding software resources and tasks

Option	Description
Add	Lets you add a software resource or a task to the delivery sequence.
Up and down arrow symbols	Let you arrange the sequence in which the software resources and tasks are run. Plan the sequence before you enable the policy. If you change the sequence after the policy runs, you trigger the following actions: ■ The policy is updated on the client computers the next time it is requested. ■ The policy's schedule is reset so that it runs again, even if you originally scheduled the policy to run one time only.

Table 7-7 Settings for software resources

Option	Description
Perform software compliance check using	Displays a link that indicates the software resource whose detection rule is used for the compliance check. You can click the link to view and edit the rule. For more information, see the topics about editing inventory rules and about detection and applicability rules in the *Symantec Management Platform Help*.
Command line	Lets you select the command line to run. This list contains all the command lines that are defined for the software resource that you selected. You can select a command line other than the default command line that appears. You can omit the command line if the package does not require one.
Package	Lets you select the package to download if the command line requires a package. The list contains all the packages that are associated with this software resource. The package that is defined in the command line is the default. You can omit the package if the command line does not require one. For example, if the command line uninstalls a package that is already on the client computer.
Advanced options	Change the settings for this software resource only. For example, you might download this software's package to a different location or allow the user to interact with this software's installation but not others.

Table 7-8 Settings for tasks

Option	Description
Override the policy settings for this task	Enables the remaining options in this section and lets you configure settings for delivering this specific task.

Table 7-8 Settings for tasks *(continued)*

Option	Description
Upon failure the Managed Delivery will	Defines whether the task aborts, continues, or restarts when it fails. When you create a Managed Software Delivery policy, this setting is the same for each task that the policy contains. You can edit the policy to override this setting for each ask. For example, if the execution of the first task fails, you can run subsequent software resource and tasks. Conversely, if one execution in the sequence fails, you can abort the remaining items in the sequence.
Terminate after	Lets you define the amount of time to wait before the task terminates if it stops responding.
Max retries	Defines the number of times that the task retries when it fails.
Show Task	Opens the task editing dialog box so you can view or edit the task. When you edit the task itself instead of its settings, any other instances of that task are also changed. For example, you create a Package Delivery task to install an FTP client and you add that task to several Managed Software Delivery policies. If you change that task in one Managed Software Delivery policy, the change affects that task as well as all the policies that contain it.

Policy Rules/Actions: Policy settings tab for Mac computers

This tab lets you change the settings for a Managed Software Delivery policy.

The following options on the **Policy Settings** tab apply to Mac computers.

Table 7-9 Options on the **Policy Settings** tab

Option	Description
Display name	Lets you define the name that appears in the Symantec Management Agent for this policy. The default name is New Managed Software Delivery. Make the name descriptive enough for users to easily identify this software.
Display description	Lets you type a description to further identify this software and make it more recognizable on the Symantec Management Agent.
Enable verbose reporting of status events	Records the details of policy status, package download, and execution events and posts them to the Notification Server computer.

About the Software Portal

The Software Portal lets users submit requests and install software through a Web-based interface with little or no administrator involvement. This self-service approach to software delivery reduces help desk calls and simplifies the process of requesting and delivering software. Because the Software Portal uses predefined software information and delivery settings, it can automate most of the deliveries that result from the software requests.

The administrator who sets up the Software Catalog decides which software each user or group of users is allowed and specifies which software requires approval. These settings determine the amount of intervention that is required for specific software requests. Requests for pre-approved software require no further action from anyone. Requests for other standard software require approval from a manager or an administrator but upon approval, the software delivery is automatic. Only the requests for non-standard software require the manager or the administrator to take further action to deliver the software.

The Software Portal is installed on the client computers. Therefore, the users can create requests and the managers can approve the requests without requiring access to the Symantec Management Console.

The Software Portal supports requests for Windows and Mac OS software.

Chapter 8

Using scripts to deliver tasks to Mac computers

This chapter includes the following topics:

- About using tasks to manage Mac computers
- About configuring a software delivery task for Mac computers
- Configuring a software delivery task

About using tasks to manage Mac computers

Apple has provided a large number of command line utilities that facilitate the management of Mac client computers. Many of these utilities have been used to create "run script" tasks in Symantec Management Console to let you run common tasks. The "run script" tasks that are available in the console let you take advantage of the built-in task server function in Symantec Management Platform. You deliver tasks to Mac computers by running these scripts.

See "About managing the Mac with CMS 7.1" on page 9.

You may want to use tasks to deliver software and to configure security; for example, to lock down a client OS. You may also want to create tasks that you can deploy for power management or to wake up and power down managed Mac computers.

To configure Mac computers using tasks, you must write scripts to execute the tasks. If this skill is unfamiliar to you, please refer to the introduction to shell scripting that is available in the Mac OS X Developer Library. Symantec has also created a set of sample scripts that you can refer to as models for creating your own scripts. These are located in the Symantec Knowledge Base, HOWTO51884.

The Symantec sample scripts are based on recommendations in these Apple Security Configuration guides.

Mac tasks fall into the following broad categories:

- Software delivery
  See "About configuring a software delivery task for Mac computers" on page 134.
- Security
- Power management.
  You can add the following tasks in the **Create New Task** window in the console under Power Control: Restart, Shut down, Log off, and Wake up
- Wake and power down

About configuring a software delivery task for Mac computers

You can deliver enterprise-class software to Mac computers using tasks that you run by creating a script.

You must follow the instructions that are found in the user guide of the software that you plan to deploy. If the software requires specific files and installers to support a silent installation, you must create them.

Ensure that you install the necessary files and installer to the correct directories. Use the exact installation path that the source media requires.

See "Configuring a software delivery task" on page 134.

Configuring a software delivery task

For any software that you want to deliver to Mac computers, you

See "About configuring a software delivery task for Mac computers" on page 134.

The process for configuring a software delivery task may vary depending on the software product that you install. The process that is laid out in the table illustrates how to install the *Adobe® Creative Suite® 4* software product. Each step links to a task that is part of this process. Because you may or may not choose to install this particular product, each task is presented as a sample.

Table 8-1 Process for configuring a software delivery task

Step	Description	Notes
Step 1	Complete software delivery prerequisites. Follow the instructions that are found in the *Adobe® Creative Suite® 4 Enterprise Manual Deployment User Guide* to create the necessary files and installer that support a silent installation. You can download the PDF can be downloaded from the Adobe site.	If you follow the instructions you produce the following required files for a silent installation: ■ application.override.xml ■ install.xml ■ remove.xml Make sure to save these files in the correct directories. The Adobe Installer appears to be hard-coded to search for certain payload items in the default path. For example, if the installer path is /Volumes/Adobe/CS4/payloads/.... but the installer looks in /Volumes/Adobe Creative Suite 4 Design Premium Disc 1/Adobe CS4 Design Premium/payloads/.... , you receive an error. When you create files or installers for the software that you want to deliver, use the exact path that the source media uses.
Step 2	Create a DMG file.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a DMG file to deliver software to Mac OS X computers" on page 136.
Step 3	Create an Installer Shell script.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating an Installer Shell script to deliver software to Mac OS X computers" on page 137.

Table 8-1 Process for configuring a software delivery task *(continued)*

Step	Description	Notes
Step 4	If the software has its own installer, import the installer into the Software Catalog.	Read through or complete a sample task and then click the link to view the next step in the process. See "Importing an installer into the Software Catalog to deliver software to Mac OS X computers" on page 138.
Step 5	If the software includes a pop-up blocker, you can create a task to disable it.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a task to disable the Product Improvement pop-up" on page 140.
Step 6	Update the Managed Software Delivery policy.	Read through or complete a sample task and then click the link to view the next step in the process. See "Creating a Managed Software Delivery policy to deliver software to Mac OS X computers" on page 140.

Creating a DMG file to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create a DMG file for installing the *Adobe® Creative Suite® 4* software product.

See "About supported package-delivery formats for software distribution" on page 14.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task" on page 134.

To create a DMG file

1. On the Mac computer, in the Finder, navigate to the folder that contains the application file.
2. Right-click the folder, and select **Get Info**.
3. Record the size of the contents.
4. In Symantec Management Console, click **Applications > Utilities > Disk Utility**.
5. Click the **New Image** icon to create a new disk image.
6. Enter a name for the image. Select an adequate size or the size of the *Adobe® Creative Suite® 4* folder.
7. Set encryption to **None** and set **Format** to **read/write disk image**.
8. Place the contents of the *Adobe® Creative Suite® 4* folder into the newly mounted disk image.
9. Unmount the disk image.

Creating an Installer Shell script to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create an Installer Shell script for installing the *Adobe® Creative Suite® 4* software product.

This task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task" on page 134.

To create an Installer Shell script

1. At the Mac Terminal, create a new shell script file and add the following line:

   ***setup.app path*/Contents/MacOS/Setup --mode=silent --deploymentFile=<install.xml or remove.xml path in quotes>**

   Refer to the following sample:

   ```
   /Volumes/Adobe/CS4/Setup.app/Contents/MacOS/Setup --mode=silent
   --deploymentFile="/Volumes/Adobe/CS4/install.xml
   ```

2. Place this file and the DMG file that you created previously into a folder.

Warning: Do not include the shell script file in the DMG. You cannot select it as the installation file if it is inside the DMG.

Importing an installer into the Software Catalog to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to import the installer for the *Adobe® Creative Suite® 4* software product into the Software Catalog.

Copy the folder structure that you created previously to the Notification Server computer file share or to another Windows file share. The Software Library has a file size limit of 2GB and cannot accommodate the typically large file size of an *Adobe® Creative Suite® 4* installer.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task" on page 134.

To import the Adobe® Creative Suite® 4 installer into the Software Catalog

1. In Symantec Management Console, click **Manage > Software Catalog**.
2. In the **Software Catalog** window, under **Deliverable Software**, click **Import** to view a model dialog box.
3. Set **Software type** to **Software Release**.
4. Set the **Package source** to match the specific type of source on which your software is hosted.

   To install the software that is referred to in this sample task, you use Access package for a directory on Notification Server.
5. Browse to the installer location and select the folder that holds the DMG and shell script files.
6. Click **Display Location** to ensure that you have selected the correct folder.

   You should see your DMG and shell script files.
7. Click your shell script file (.sh) and then click **Set Installation File**.

   Caution: If you fail to set the installation file in this step, you cannot create command lines later.
8. Click **Next**.
9. Click **Create a new software resource**.
10. Give this software a meaningful name (for this sample task, a meaningful name is Adobe Creative Suite 4 Design Premium.
11. Set **Company** to Adobe Systems

12 Set **Version** to 4 or other specific version of the software that you choose to install.

13 Leave **Open software resource for editing when finished** selected.

Note: If you have a pop-up blocker enabled, disable it. A pop-up blocker prevents a new window from opening. if the window is blocked, locate the software in the list, highlight it, and click **Edit** (the pencil icon).

---

14 On the **Properties** tab, **Software Product** may be blank.

You can create a new Software Product named **Creative Suite**.

15 Click the **Package** tab.

A package was already created. However, a command line may not be there.

16 Click **Add command**.

17 In **Name** enter **Install**.

Description is optional.

18 Leave **Command line requires a package** selected.

The Adobe CS4 package should be selected by default.

19 In the **Package** field, your Adobe CS4 package should be selected by default.

20 Set the Installation file type to <other>.

21 Set the Command type to Install.

22 Click **Set** as the default for this command type.

23 Click **Edit** for the Command line.

24 Click the **.sh** file and then click **OK**.

The resulting command line should be `NameOfYourFile.sh`

25 Set the following **Success Codes**: 0, 8 (comma delimited)

26 Set **Failure Codes** to 1, 2, 6, 7, 9, 10, 11, 12, 13, 14.

These codes are specific to Adobe® Creative Suite® 4. Refer to the product PDF for details if you install this software product. If you follow the instructions in this sample task to install a different software product, refer to the product information for the failure codes.

27 Click **OK** and close the window.

Creating a task to disable the Product Improvement pop-up

(Sample)

This sample task illustrates how to disable the Adobe Product Improvement pop-up. This task runs after the *Adobe® Creative Suite® 4* software installation to disable the pop-up for new users.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task" on page 134.

To create a task to disable the Product Improvement pop-up

1. In Symantec Management Console, navigate to **Manage > Jobs and Tasks**
2. At the root of this folder, create a folder to work in.
3. Right-click the new folder and click **New > Task**.
4. Click **Run Script** to select that task type.
5. Give the task a descriptive name.

   You can use any descriptive name such as **Disable Adobe Product Improvement Program**.
6. Set the script type to UNIX Script.
7. Add the following string to the body:

   ```
   defaults write /Library/Preferences/com.adobe.headlights.APIP
   Enabled -int 0
   ```
8. Click **OK** to save the task.

Creating a Managed Software Delivery policy to deliver software to Mac OS X computers

(Sample)

This sample task illustrates how to create a Managed Software Delivery policy for installing the Adobe® Creative Suite® 4 software product.

This sample task is a step in the process for configuring a software delivery task.

See "Configuring a software delivery task" on page 134.

To create a Managed Software Delivery policy

1. In Symantec Management Console, click **Manage > Policies**.
2. Click **Policies > Software > Managed Software Delivery**.

3 Right-click the **Managed Software Delivery** folder and click **New > Managed Software Delivery**.

4 Click the **New Managed Software Delivery** title and enter a descriptive name, or add an entry in the **Description** field.

5 Under **Policy Rules/Settings**, on the **Software** tab, click **Add > Software Resource**.

6 Select the software resource that you created previously, and click **OK**.

7 In the right pane, ensure that **Install Command** line and the correct CS4 software package are selected.

8 Click **Add > Task**.

9 Navigate to the **DisableAdobeProductImprovementProgram** task that you created earlier, highlight it, and click OK.

The task type is **Run Script**.

10 In the distribution tree, ensure that the task appears after the software.

11 On the **Policy Settings** tab, enter a meaningful display name.

You can include a description if you want to.

12 (Optional) On the **Software Publishing** tab, make this software available for users through the Software Portal.

13 On the far right in the **Policy Rules/Actions** area, click the Up arrow to collapse the section.

14 In the **Applied to** area, click **Apply to > Computers** to select the computers to which you want to apply this policy.

15 Beginning with all resources, click **Add rule** to filter out the computers to which you do not want to apply this policy.

16 Click **Add rule** again and continue to refine the results.

Refine the results until you are confident that you have applied this policy to the Mac computers for which you intend the policy.

As you refine the results, click **Update results** to list the resources that this policy targets.

Continue to filter the resource target so that it contains the exact subset of Mac computers to which you want the policy to apply.

17 Click **OK**.

18 Click the Up arrow on the right to collapse this area.

19 Click **Add schedule** to select a time to install the software.

Leave the **Remediation** option set to **Immediately**.

20 Save changes.

21 To turn on the policy click the red circle next to the **Off** label, click **On**, and click **Save**.

The software installs silently at the selected installation time.

Chapter 9

About Mac Patch Management

This chapter includes the following topics:

- About patching Mac software
- About how Mac patching works
- About hosting an internal SUS to obtain internal software updates
- Redirecting a Mac client computer to a local SUS

About patching Mac software

Patching software to keep it up to date is a common administrator task. In the Mac world, you run a software update utility.

See "About managing the Mac with CMS 7.1" on page 9.

To keep software on Mac computers up to date, you run a scheduled client task on each Mac. This task invokes the local software update utility, `softwareupdate -l` (the letter ell stands for the word local). This utility finds the software that is available for installation. When you run the `softwareupdate -l` command, you see a list of applicable updates.

The software update utility passes results back to Notification Server for central reporting, and the results are stored in the Configuration Management Database (CMDB).

You can update the software in the following ways:

- Use Task Server to selectively schedule the installation of one or many software updates.

Some updates require a restart. When you schedule updates with Task Server, you can allow end-user notifications so that users are aware that updates need to be installed.
In Symantec Management Console, under the **Reports** menu, you can get a list of which computers require a restart.

- Run pre-built jobs out of box to enable automatic patching.

About how Mac patching works

All Mac computers need to have direct Internet access. All Mac computers download updates from Apple.com.

Without allowing Mac client computers Internet access, the only way you can still patch Mac software is to use a Software Update Server (SUS). In this case, you must redirect all clients to the SUS on the Mac OS X server.

Software Update Server is part of the OS X Server operating system and contains a repository of all available updates. The OS X Server must be connected to the Internet to download Apple updates. Mac clients can then be redirected to the SUS service on the OS X Server.

The Software Update utility is built in to each client Mac. Users can run the `softwareupdate` command from time to time or on a schedule like a Windows scheduled task.

If a Mac client has Internet access, then the user can update software. The software update utility runs on the Mac client and presents available services or updates. The user selects the desired services or updates, which are then downloaded through the GUI on the client.

About hosting an internal SUS to obtain internal software updates

You can allow Mac client computers direct access to the Apple software update site or host a Software Update Server (SUS) internally.

See "Redirecting a Mac client computer to a local SUS" on page 145.

Symantec recommends that you allow direct client access to the Apple software download site rather than setting up a SUS.

Hosting a SUS is a task for advanced Mac administrators because setup is somewhat complex. Setup requires that you change settings manually on every Mac client. To simplify the process, you can create an image, install it on all Mac computers, and then run scripts to change the settings.

The benefit to hosting a SUS internally is that you download software updates from Apple one time and then distribute software updates over the network. This method is more secure and requires lower bandwidth than having Mac clients download software directly over the Internet.

Note that a SUS is not part of Symantec Management Platform or CMS; however, you can host it on the same network. See Management scripts, including setting liveupdate server (SUS) and Mac SUS server setup.

Redirecting a Mac client computer to a local SUS

Symantec recommends that you allow direct client access to the Apple software download site. An alternative is to set up a Software Update Server (SUS), which is complex and requires substantial manual configuration.

Although it is not recommended that you configure a local Software Update Server (SUS) to manage Apple software updates, it can be done. After you configure the SUS, the Altiris Patch Management for Mac 7.1 from Symantec solution then pulls the software updates locally. This method can be more efficient and require fewer network resources than allowing every Mac client to pull updates individually from the Apple Web site .

See "About hosting an internal SUS to obtain internal software updates" on page 144.

If you decide to redirect a Mac client to a local SUS, the option you choose depends on which user or users should be affected. It also depends on which tool should be affected, such as GUI or command line utility.

Note: The port specification is required only if your update server uses a port other than the default port or ports.

You can direct client back to Apple rather than the local Software Update Server. To redirect a client, you remove the preference setting that points to an internal server. In this case, you have two options. You can delete the modified setting and allow the client computer to revert to Apple for software updates. Another option is to remove the preference settings altogether by deleting the files from both the user's home folders and the root home folder.

Redirecting a Mac client computer to a local SUS

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Update the preference setting for the user or group by executing the relevant command:

The local user who is running the command updates own preference setting. This method only affects the GUI Software Update tool.	`defaults write com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`
You (the administrator) update the global settings for all users on a system. This method only affects the GUI Software Update tool.	`defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`
The root user (a local user using `sudo` to get administrator privileges) updates own global settings. This method affects the command-line softwareupdate utility.	`sudo defaults write com.apple.SoftwareUpdate CatalogURL "http://update.server.address:8088/"`

To remove the preference settings and allow the client computer to revert to Apple for software updates

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Perform an appropriate `defaults read` action to validate the information to be deleted.

   You can execute the `defaults read` command to make sure that you do want to delete the information that you are about to delete.
3. Remove the settings using one of the following commands:

The local user who is running the command removes own settings.	`defaults delete com.apple.SoftwareUpdate CatalogURL`
You (the administrator) update the global settings for all users on a system.	`defaults delete /Library/Preferences/com.apple.SoftwareUpdate CatalogURL`
The root user.	`sudo defaults delete com.apple.SoftwareUpdate CatalogURL`

To remove the preference settings

1. On the Mac client computer, click **Finder > Applications > Utilities > Terminal.app** to open a Terminal window (command prompt).
2. Remove the softwareupdate configuration for the account in one of the following ways:

   If you set up the SUS from a user's account, then you should remove it from that account using the `rm ~/path` command. Adding the tilde (~) means "Go to this user's account." This command lets you delete the account for the current user.

The root account.	`rm /Library/Preferences/com.apple.SoftwareUpdate.plist`
Individual user account.	`rm ~/Library/Preferences/com.apple.SoftwareUpdate.plist`

Chapter 10

Patch Management Solution for Mac

This chapter includes the following topics:

- About Patch Management Solution for Mac
- Implementing Patch Management Solution for Mac
- Checking for available software updates
- Viewing the list of available software updates
- About installing software updates
- Installing individual software updates
- Installing all updates
- Patch management for Mac return codes
- About Patch Management Solution for Mac reports
- Viewing reports
- About the Mac compliance dashboard

About Patch Management Solution for Mac

Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed software updates. You can distribute all or some of the updates.

Patch Management Solution for Mac can update only the software that the Mac OS X software update utility supports. The solution integrates with the software update utility, and lets you collect needed update information from the target Mac computers and initiate a software update. Mac computers download software updates from the Apple Web site or from a Software Update Server (SUS) and report installation status information to Notification Server.

Patch Management Solution for Mac provides the preconfigured rollout jobs that let you automate installing a large number of updates. For example, the preconfigured rollout jobs can install all updates, all recommended updates, and so on.

See "Implementing Patch Management Solution for Mac" on page 150.

Implementing Patch Management Solution for Mac

The recommended workflow for updating Mac computers is as follows:

See "About Patch Management Solution for Mac" on page 149.

Table 10-1 Process for implementing Patch Management Solution for Mac

Step	Action	Description
Step 1	Install or upgrade the solution.	Use Symantec Installation Manager to install the solution.
Step 2	Install or upgrade the Symantec Management Agent.	Install or upgrade the Symantec Management Agent for UNIX, Linux, and Mac on the target Mac computers. See "About installing the Symantec Management Agent for UNIX, Linux, or Mac" on page 20.

Table 10-2 Process for installing software updates

Step	Action	Description
Step 1	Check for available updates.	You can check target Mac computers for the software updates that they require. See "Checking for available software updates" on page 151.
Step 2	Install all or some of the updates.	You can install individual updates or use batch rollout jobs. See "About installing software updates" on page 152.

Table 10-2 Process for installing software updates *(continued)*

Step	Action	Description
Step 3	View installation status reports.	Use reports to view the software update compliance and rollout job status. See "Viewing reports" on page 156.

Checking for available software updates

You can check target Mac computers for the software updates that they require. When you run the **Check Available Updates Task**, the target Mac computers download software update information from Apple and then report the list of available updates to Notification Server.

To ensure that the list of available software updates on Notification Server is kept up-to-date, schedule the task to run twice a week. Configure the task to run on the **All Patchable Mac Computers** target.

If you want to quickly check Mac computers for compliance, you can run the task immediately.

After you collect software update information from Mac computers, you can view this information in reports.

See "Viewing the list of available software updates" on page 152.

See "Implementing Patch Management Solution for Mac" on page 150.

To check for available software updates

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **System Jobs and Tasks > Software > Patch Management > Mac**, and then click **Check Available Updates Task**.
3. Under **Task Status**, click **New Schedule**.
4. Under **Schedule**, do one of the following:
   - If you want to run the task immediately, click **Now**.
   - If you want to schedule the task, click **Schedule**, and then configure the schedule. Symantec recommends that you schedule this task to run twice a week.
5. Under **Input**, click **Add > Target**.
6. Click **Open**.

7 In the **Open** dialog box, click **All Patchable Mac Computer Target**, and then click **OK**.

8 Click **OK**.

9 Click **Schedule**.

Viewing the list of available software updates

You can view the list of available software updates in the **Available Mac Software Updates for computers managed by this server** report. The report also shows the number of computers that require an update.

In reports, you can drill down on specific items to obtain additional information.

To populate the report, collect the available software updates inventory.

See "Checking for available software updates" on page 151.

See "Implementing Patch Management Solution for Mac" on page 150.

To view the list of available software updates

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Software > Patch Management > Mac**, and then click **Available Mac Software Updates for computers managed by this server**.

About installing software updates

With Patch Management Solution for Mac, you can use the following methods of installing software updates:

- Install individual software updates.
  See "Installing individual software updates" on page 152.
- Install all updates that match specific criteria using automated rollout jobs.
  See "Installing all updates" on page 154.

See "Implementing Patch Management Solution for Mac" on page 150.

Installing individual software updates

You can install individual software updates directly from reports.

Before you can install updates, you must collect available software updates inventory.

See "Checking for available software updates" on page 151.

To install software updates, you create a software update rollout job. You can view the rollout jobs and their status at **Manage > Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Mac > Rollout Jobs**.

If you want to install multiple updates at a time, Symantec recommends that you combine them in one rollout job rather than installing each update on an individual schedule. This ensures that package downloads and restarts are not interfering each other.

See "About installing software updates" on page 152.

See "Implementing Patch Management Solution for Mac" on page 150.

To install individual software updates

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, click **Software > Patch Management > Mac > Available Mac Software Updates for computers managed by this server**.
3. Click the updates that you want to install.

   To highlight multiple items, hold down the Ctrl or Shift key.
4. Right-click the selected updates and then click **Create Rollout Job**.
5. (Optional) In the dialog box that opens, modify the name and the description of the rollout job that you just created.
6. Under **Task Status**, click **New Schedule**.
7. In the **New Schedule** dialog box, configure a schedule for this software update rollout job.

   For example, click **Now**.
8. Under **Input**, click **Add > Target**.
9. In the **Add Target** dialog box, click **Open**.
10. In the **Open** dialog box, click **All Patchable Mac Computers Target** and then click **OK**.

    It is safe to run the rollout job on all supported Mac computers. When the rollout job runs, it checks if the update that you want to install is needed. If the update is not needed, the job does not download and does not install the update.
11. Click **OK**.

12 Click **Schedule**.

13 Close the dialog box.

Installing all updates

Patch Management Solution for Mac also provides the automated rollout jobs that let you install all software updates that match a specific criteria. For example, you can choose to install all available updates, all recommended updates, all updates that do not require a restart, and so on.

To ensure that Mac computers in your environment are always up-to-date, you can configure automated rollout jobs to run on a schedule. For example, you can configure the jobs to run weekly.

See "About installing software updates" on page 152.

See "Implementing Patch Management Solution for Mac" on page 150.

To install all updates

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, expand **System Jobs and Tasks > Software > Patch Management > Mac > Automated Rollout Jobs**.

3 Click the rollout job that you want to run.

4 In the right pane, under **Task Status**, click **New Schedule**.

5 In the **New Schedule** dialog box, configure a schedule for this automated rollout job.

For example, configure the job to run weekly.

6 Under **Input**, click **Add > Target**.

7 In the **Add Target** dialog box, click **Open**.

8 In the **Open** dialog box, click **All Patchable Mac Computers Target** and then click **OK**.

It is safe to run the rollout job on all supported Mac computers. When the rollout job runs, it checks which updates are needed. If no updates are needed, the job does not download and does not install any updates.

9 Click **OK**.

10 Click **Schedule**.

Patch management for Mac return codes

When you run client tasks within the default rollout jobs that are created with Patch for Mac, you can expect to see certain return codes. If you need to do some troubleshooting, the information in the following quick-reference table can help you interpret what the codes mean. The table lists return values and their meanings. The information in the table was reproduced from a Symantec Connect blog post. View the Symantec Connect blog post here.

0	Installation finished successfully
1	Installation finished successfully Restart required
2	Update installation failure
3	Update installation failure Restart required
4, 127	Invalid command line options
5	`softwareupdate` utility failure
6	Error parsing output of `softwareupdate` utility
7	Error communicating with Symantec Management Agent

About Patch Management Solution for Mac reports

Patch Management Solution for Mac provides you with reports that let you view the software update compliance and rollout job status.

See "Viewing reports" on page 156.

Table 10-3 Patch Management Solution for Mac reports

Report	Description
Available Mac Software Updates for computers managed by this server	Displays the list of software updates that the target Mac computers require. To populate this report, you must run the **Check Available Updates Task**. See "Checking for available software updates" on page 151. You can create software update rollout jobs and install updates directly from this report. See "Installing individual software updates" on page 152.
Mac Software Update Compliance	Displays the percentage of computers that require an update. To populate this report, you must run the **Check Available Updates Task**. See "Checking for available software updates" on page 151.
Mac Software Update Installation Status	Displays the software update rollout job status. The number in the **Succeed** column indicates the number of times the job has run, regardless of whether the update was needed. See "Installing individual software updates" on page 152.

Viewing reports

Patch Management Solution for Mac reports let you view the software update compliance and rollout job status.

See "About Patch Management Solution for Mac reports" on page 155.

See "Implementing Patch Management Solution for Mac" on page 150.

To view Patch Management Solution for Mac reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Software > Patch Management > Mac**.
3. Click the report that you want to view.

About the Mac compliance dashboard

This portal page provides patch management summary information at a glance. The page is comprised of a number of Web parts displaying results from commonly used reports.

See "About Patch Management Solution for Mac reports" on page 155.

You can access the home page by clicking **Home > Patch Management**, and then, under **Mac OS X**, clicking **Compliance Dashboard**.

Table 10-4 Web parts on the **Mac Software Update Compliance Portal** page

Report	Description
Getting Started	Displays the recommended Patch Management Solution for Mac implementation workflow.
Mac Software Update Compliance	Reports the number of Mac computers that require or do not require an update.
Mac Software Update Delivery Summary	Displays the list of software update rollout jobs and the number of computers that succeeded or failed to run the job.

Chapter 11

Remote control with Mac computers

This chapter includes the following topics:

- About remote control with the Mac
- pcAnywhere communication requirements
- pcAnywhere Connection tab
- pcAnywhere Authentication tab
- pcAnywhere Access Server tab
- Installing the pcAnywhere plug-in

About remote control with the Mac

Altiris Client Management Suite 7.1 from Symantec includes pcAnywhere Solution, which lets you remotely control Windows, Mac, and Linux computers from Symantec Management Console.

Remote control is the primary function that the Mac thin host provides. pcAnywhere also provides a default level of encryption.

The pcAnywhere product supports a subset of functions for non-Windows systems, as follows:

- Authentication
  Authentication refers to the requirement for remote users to specify valid credentials before the pcAnywhere host program allows a remote-control session.
- Access Server

For information about pcAnywhere and Access Server, including links to relevant documentation, see Questions and Answers about pcAnywhere Access Server.

- Screen scaling
  Screen scaling is useful when the host computer screen resolution is higher than the resolution of the remote computer screen. In this scenario screen scaling lets the remote user see the entire host computer screen without using scroll bars.
- Session Recording
  If you need to record a remote session, use the **Start Recording** option on the remote computer. After the remote user specifies a path name and file name where the recording is to be saved, recording begins.
- Snapshots
  To save a local screen shot of the display on the host computer, click the **Take Snapshot** button in the pcAnywhere program on the remote computer. This action is recommended over using the computer's **Print Screen** button.

If you want to remotely control the Mac computers on your network in Symantec Management Console, you must turn on the **pcAnywhere Solution Plug-in for Mac - Install** policy. You use pcAnywhere Solution when you need to remotely control the console session of a Mac server or workstation.

See "Installing the pcAnywhere plug-in" on page 163.

Caution: Before you initiate a remote session, you must log on directly to the Mac that you intend to remotely control. After you have logged on to that computer, you can connect to it from Symantec Management Console with the **Remote Control** action. Failure to log on directly to the Mac before you initiate a remote session causes problems. For details, refer to the Symantec Knowledge Base, TECH127293, "KNOWN ISSUE: pcAnywhere for Mac requires that a user be logged on.".

Refer to the following terms to prevent confusion:

console	The browser that connects to the host

thin host	The pcAnywhere program running on a managed Mac This program makes the managed Mac the host. This host Mac is the computer that is remotely controlled; in other words, it hosts the remote control session. The program is commonly referred to as thin host for two reasons: it has a relatively small footprint, and it provides a subset of features that are available with the pcAnywhere program for Windows. The thin host listens for remote control requests, authenticates remote control users, and provides remote control. The thin host runs as a service and continues to run even if the Symantec Management Agent is stopped. This ensures the ability to remotely control a computer even if the agent is stopped or fails.
pcAnywhere plug-in	The plug-in to Symantec Management Agent This plug-in runs on the managed Mac and communicates with Symantec Management Agent and the Mac host. The plug-in is also responsible for the logging that gets sent back to Notification Server and is used for reporting.

Before you attempt to use pcAnywhere solution, ensure that your protocols and ports meet the pcAnywhere communication requirements.

See "pcAnywhere communication requirements" on page 161.

pcAnywhere communication requirements

The table lists the required ports and protocols.

See "About remote control with the Mac" on page 159.

Table 11-1 pcAnywhere communication requirements

Component	Ports	Protocols	Administrator can change the setting (Y/N)
thin host	5631 5632	TCP UDP	No

pcAnywhere Connection tab

In Symantec Management Console, under **Settings > Agents/Plug-ins > Remote Management**, expand the Mac folder and click **pcAnywhere Settings - Mac**. You

can then click the **Connection** tab and select options depending on what you want to accomplish.

See "About remote control with the Mac" on page 159.

Require user to approve connection	A user in this case means the person who operates the Mac client computer. When you enable this option, you as the administrator cannot remotely control that client until the user approves.
Use encryption (Symmetric AES 128-bit)	When you enable this option, the data stream between the remote computer and the host computer is encrypted. The remote computer is Symantec Management Console. The host computer is the Mac client that runs the thin host.

pcAnywhere Authentication tab

In Symantec Management Console, under **Settings > Agents/Plug-ins > Remote Management**, expand the Mac folder and click **pcAnywhere Settings - Mac**. You can then click the **Authentication** tab and select options depending on what you want to accomplish.

See "About remote control with the Mac" on page 159.

Authentication	Two types are available, as follows: ■ **pcAnywhere** If you use pcAnywhere authentication, in the **Active users or groups** area you can click **Add** to specify one user and a password. ■ **Open Directory** If you use Open Directory authentication, you cannot add a user. The operating system controls who can authenticate with Open Directory credentials.

pcAnywhere Access Server tab

In Symantec Management Console, under **Settings > Agents/Plug-ins > Remote Management**, expand the Mac folder and click **pcAnywhere Settings - Mac**. You

can then click the **Access Server** tab and select options depending on what you want to accomplish.

Select options on the **Access Server** tab depending on what you want to accomplish.

See “About remote control with the Mac” on page 159.

If you need information about pcAnywhere Access Server, refer to the following documents:

- "Symantec pcAnywhere Access Server Implementation Guide," DOC1842 in the Symantec Knowledge Base
- "Questions and Answers about pcAnywhere Access Server," HOWTO10840 in the Symantec Knowledge Base

Installing the pcAnywhere plug-in

To control managed Mac computers remotely, you must install the pcAnywhere (pcAnywhere) plug-in. Installing the pcAnywhere plug-in provides communication between Symantec Management Agent on the managed Mac and Notification Server.

See “About remote control with the Mac” on page 159.

You can install the plug-in by policy or manually. Installing the pcAnywhere plug-in by either method requires that you re-enable the root user if you had explicitly disabled it previously. To install the plug-in manually, enable the root user and then copy and execute the installation program.

Installing the plug-in by policy is like installing any other plug-in and includes turning on the plug-in installation policy in Symantec Management Console. Enable the root user, and then turn on the policy.

The following procedure comes directly from the article titled How to manually install the pcAnywhere Solution agent on a Macintosh. Click the link to ensure that you have the latest steps.

See “About remote control with the Mac” on page 159.

To enable the root user and install the pcAnywhere plug-in

1. On the Mac client computer, on the **Apple** menu, select **System Preferences...**.
2. On the **View** menu, select **Accounts**.
3. Click the **lock** and authenticate, using an administrator account.
4. Click **Login Options...**.

5 At the bottom right, click **Edit...** or **Join...**.

6 Click **Open Directory Utility...**.

7 In the **Directory Utility** window, click the **lock**.

8 Enter an administrator account name and password, and click **OK**.

9 On the **Edit** menu, select **Enable Root User**.

10 In both the **Password** and **Verify** fields, enter the root password you want to use, and click **OK**.

11 On the **Apple** menu, if you are logged in, select **Log Out**.

12 If you log in from a list of user names with pictures, click **Other**.

13 In the **Name** field, enter `root`.

14 In the **Password** field, enter the password that you defined in the preceding steps.

15 Copy and execute the installation program (the host).

See "Copy and execute the installation program for a manual plug-in installation" on page 164.

Copy and execute the installation program for a manual plug-in installation

1 After you enable the root user, in Symantec Management Platform copy the entire **NSCap\bin\Win32\X86\pcAMacAgent** folder to the managed Mac to copy all the installation files.

See "To enable the root user and install the pcAnywhere plug-in" on page 163.

2 On the managed Mac, open the **Terminal** and change the path to the folder where you copied the installation files.

Use the `cd` command.

3 Run the following command:

```
sudo sh Rollout_mac.sh -install
```

Note: If you do not have root privileges, use the `sudo` command, as follows:

```
sudo sh Rollout_mac.sh -install
```

---

4 Ensure that the agent has sent an inventory and has the pcAnywhere settings that are specific to your environment.

5 If the installation program, or host, does not start automatically, follow these steps:

Change the folder path.	On the managed Mac, open the **Terminal** and change the folder path to **MacHD/opt/altiris/notification/SymantecpcAPlugin/bin**.
Start the host.	On the managed Mac, run the following command: `./Thinhost`

To turn on the pcAnywhere Solution plug-in for Mac by policy

1 In Symantec Management Console, click **Settings > Agents/Plug-ins > Remote Management > Remote Control**, and expand **Mac**.

2 Under **Mac**, select **pcAnywhere Plug-in for Mac - Install**.

3 Turn on the policy and then save changes.

Appendix A

Mac imaging

This appendix includes the following topics:

- About setting up the Mac imaging environment
- System requirements for Mac imaging in Deployment Solution 6.9
- About the limitations of imaging Mac computers
- About using Deployment Solution 6.9 to manage and image Mac computers
- Using Deployment Solution 6.9 to manage Mac computers
- Using Deployment Solution 6.9 to image Mac computers
- Performing management tasks
- About Installing Mac OS X Server software
- Creating a Mac OS X automation image
- Installing Mac OS X
- Customizing the source OS
- Installing the Darwin ADLagent
- Enabling Darwin ADLagent logging
- Converting the Darwin ADLagent to an automation role
- Adding Share credentials to the source keychain
- Capturing the source image
- Creating the NetBoot image using the System Image Utility
- Setting up the NetBoot service

- Performing imaging tasks

About setting up the Mac imaging environment

If you need to capture and deploy Mac images, you need the information in this appendix. If you only need to discover and manage Mac computers (Mac computers) in your network, you do not need the information in this appendix.

See "About managing the Mac with CMS 7.1" on page 9.

The information in this appendix guides you through capturing and deploying a standard Mac image or a corporate Mac image. You can then use the image with Mac computers on your network. Links to relevant Apple documentation are included.

Caution: Although you can use other methods to image Mac computers, Symantec supports only the method that is presented in this guide.

The first step for imaging Apple systems is to create a Mac OS X automation environment.

This process is different from Windows and Linux imaging, for which Symantec provides preboot environments such as WinPE and Linux, and requires two distinct components: the first component of the Mac automation environment is an Apple server running a licensed copy of Mac OS X Server. The Mac OS X Server is a prerequisite for the second component, which is a NetBoot image. Neither Apple nor Symantec provides this image out of the box.

See "System requirements for Mac imaging in Deployment Solution 6.9" on page 169.

When running Altiris Client Management Suite (CMS) 7.1 from Symantec, you must use Deployment Solution 6.9 to capture and deploy Mac images. Deployment Solution 6.9 requires that you possess a licensed copy of Mac OS X Server. The Mac OS X Server software includes a NetBoot server service. The NetBoot server service is a critical component of the Mac imaging process in Deployment Solution 6.9.

The Deployment Solution 6.9 imaging process lets you capture and deploy the Mac images. The NetBoot service of Mac OS X Server functions equivalently to the PXE service that is used for imaging Windows computers. That is, NetBoot is a method by which you can boot a Mac client into an automation environment. Note that in the Deployment Solution 6.9 imaging process, the terms *creating* and *capturing* are used interchangeably for all platforms.

Note that Symantec supports only the NetBoot service that is included with Mac OS X Server. You see references in this appendix to the Mac OS X (NetBoot) server to clarify that the NetBoot service performs a given function.

Using the NetBoot service, users can boot into a diskless state to allow for imaging of their hard drive. By default, Apple computers are not configured to boot through NetBoot. Unless you have specified a NetBoot image as the default startup disk, the client Mac computer first attempts to boot from the hard drive. The instructions for modifying the boot order are documented in this appendix.

The ability to image Mac clients with Deployment Solution 6.9 is not available out of the box. You must perform an additional configuration step after you install Deployment Solution 6.9, before you can image Mac clients: You must create a Mac OS X automation environment. After you configure the automation environment, you have the equivalent functionality of a Windows pre-boot environment. You can then capture and deploy Mac images.

See "About the limitations of imaging Mac computers" on page 171.

After you have configured the imaging capability, any Mac that boots through NetBoot boots from the automation image. This image contains the Deployment Solution Darwin ADLagent which checks in with the Deployment Server and enables management of the Mac client in the Deployment Console.

This appendix guides you through creating and deploying a Mac OS X automation image for use with Deployment Solution 6.9. Symantec does not assume that you are familiar with Mac OS X or Mac concepts generally. Consequently, links to online resources are provided to assist you with unfamiliar tools such as the vi text editor. Mac OS X Server is the only supported NetBoot server for use with Symantec Deployment Solution 6.9. For purposes of Mac imaging, the terms *Mac OS X Server* and *NetBoot server* are interchangeable; however, this appendix uses the term *Mac OS X Server*.

See "Performing imaging tasks" on page 190.

System requirements for Mac imaging in Deployment Solution 6.9

Ensure that you have the required hardware and software installed before you begin to create or deploy a Mac OS X automation image.

See "About setting up the Mac imaging environment" on page 168.

Symantec recommends the following system requirements:

Deployment Agent (DarwinADLAgent)	Deployment Agent requires network connectivity and around 32 MB disk space. Other system requirements are the same as the host operating system.
Deployment Server	Your CMS installation includes Deployment Solution 7.1. If you purchased licenses for Deployment Solution 7.1, you also have licenses for the Deployment Solution 6.9 product. Note that Deployment Solution 6.9 is a separate, standalone product that you must install. Read about Deployment Solution 6.9 platform support in the Symantec knowledge base article number HOWTO48932 titled "Deployment Solution 6.9 SP5 Supported Platforms and System Requirements." Run Deployment Server on a modern, dedicated server with a 1 GHz or faster processor with 1 GB or more of RAM. A minimum is a PIII-compatible 600 MHz or newer processor with 512 MB RAM. See "About using Deployment Solution 6.9 to manage and image Mac computers" on page 172.
Automation	Mac OS X Server v10.5 or greater running the NetBoot server service. Mac clients are compatible with NetBoot and meet its minimum requirements.

For the Deployment Solution database, see the system requirements and guidelines for the database version that you run.

Table A-1

Component	Software	Hardware
Apple Mac OS X Server	Install a licensed copy of one of the following versions of Mac OS X Server software on the required hardware: ■ Mac OS X Server 10.5 Leopard ■ Mac OS X Server 10.6 Snow Leopard For installation help, see the relevant Apple OS X Server installation guide.	Use the hardware that Apple requires for running the software version you choose.

Table A-1 *(continued)*

Component	Software	Hardware
Microsoft Windows Server running Deployment Solution 6.9	Install Deployment Solution 6.9 on your CMS server or a dedicated Windows server. For details about Deployment Solution 6.9 supported platforms through SP5, see the Symantec knowledge base article number HOWTO48932 titled "Deployment Solution 6.9 SP5 Supported Platforms and System Requirements."	For details about Deployment Solution 6.9 supported hardware through SP5, see the Symantec knowledge base article number HOWTO48932 titled "Deployment Solution 6.9 SP5 Supported Platforms and System Requirements."
Apple Mac OS X Client	Install one of the following versions: ■ Mac OS X 10.3 Panther ■ Mac OS X 10.4 Tiger ■ Mac OS X 10.5 Leopard ■ Mac OS X 10.6 Snow Leopard	Dedicated Mac computer on which to build the automation image. Use the hardware that Apple requires for running the software version you choose.

About the limitations of imaging Mac computers

Imaging Mac computers initially requires more work than imaging Windows clients. This extra work is due mainly to preparing an automation environment. After you have followed the steps in this appendix to create a Mac OS X automation environment, you can skip these steps for all future imaging tasks. Running imaging jobs is identical to running Windows imaging jobs.

After you install Deployment Solution 6.9, you must create an automation image before you can create or deploy Mac images. Creating an automation image requires that you dedicate a Mac computer to this purpose temporarily.

See "About setting up the Mac imaging environment" on page 168.

Table A-2 Limitations of imaging Mac computers

Feature or requirement	Mac imaging	Windows imaging
Dual boot imaging	Not available	Available

Table A-2 Limitations of imaging Mac computers *(continued)*

Feature or requirement	Mac imaging	Windows imaging
Deployment Solution 6.9	Yes. Deployment Solution 6.9 is required for imaging Mac computers.	Not required

About using Deployment Solution 6.9 to manage and image Mac computers

If your network includes Mac computers and you want to image them, you must use Deployment Solution 6.9. This software lets you image your production Mac computers.

See "Using Deployment Solution 6.9 to manage Mac computers" on page 172.

See "Using Deployment Solution 6.9 to image Mac computers" on page 174.

Your Altiris Client Management Suite 7.1 from Symantec product includes Deployment Solution 7.1. If you purchased licenses for Deployment Solution 7.1, you have the licenses you need to download and use Deployment Solution 6.9. If you have not yet downloaded and installed Deployment Solution 6.9, you must do that before proceeding. You can install Deployment Solution 6.9 on a dedicated server or on the same server where you have CMS installed.

Caution: In either case, do not install PXE components.

Select an installation location depending on your needs, as follows:

- If you want to use the full functionality of Deployment Solution 6.9 to manage and image production Mac computers, install Deployment Solution 6.9 on a dedicated server.
- If you only want to image Mac computers, you can install Deployment Solution 6.9 on the same server where CMS 7.1 is installed.

Using Deployment Solution 6.9 to manage Mac computers

This topic presents the process for managing Mac computers separately from imaging Mac computers. If you plan to manage and image Mac computers using

Deployment Solution 6.9, you must complete all the steps in each process. If you plan to image (but not manage) Mac computers using Deployment Solution 6.9, follow the process for imaging Mac computers.

See "About using Deployment Solution 6.9 to manage and image Mac computers" on page 172.

See "Using Deployment Solution 6.9 to image Mac computers" on page 174.

Table A-3 Process for managing Mac computers with Deployment Solution 6.9

Step	Action	Description
Step 1	Install the Deployment Solution agent (Darwin ADLagent).	Install the Darwin ADLagent. You install this production agent on a managed Mac client computer. You can then use the available Deployment Solution 6.9 tasks with that computer. A change was made in Mac OS X build 10.5.4 (Leopard). This change prevents the ADLagent installer from prompting the user for the IP addresses of the Deployment and NetBoot servers during installation. This problem was resolved in Mac OS X v10.6 (Snow Leopard). If you run any version of Mac OS X between 10.5.4 and 10.5.8, please refer to Symantec Knowledge Base article TECH41162 for more information. See "Installing the Darwin ADLagent" on page 184.

Table A-3 Process for managing Mac computers with Deployment Solution 6.9 *(continued)*

Step	Action	Description
Step 2	Perform management tasks.	You can perform management tasks as follows: ■ Run the built-in **Power Control** tasks: **Restart**, **Shutdown**, **Wake-Up**. ■ Use the **Run Script** task. This task contains a script that the target computer runs. You use scripts to run any task you choose. If you are familiar with creating Linux or UNIX scripts, you may know how to write scripts for Mac. If you need help with scripts, refer to the Apple Developer Connection (ADC) site. Note that you do not need to have a developer account to access this site. ■ Run the **Copy File to....** Task. See "Performing management tasks" on page 176.

Using Deployment Solution 6.9 to image Mac computers

This topic presents the process for imaging Mac computers separately from managing them. If you plan to manage and image Mac computers using Deployment Solution 6.9, you must complete all the steps in each process. If you plan to manage (but not image) Mac computers using Deployment Solution 6.9, follow the process for managing Mac computers.

See "About using Deployment Solution 6.9 to manage and image Mac computers" on page 172.

See "Using Deployment Solution 6.9 to manage Mac computers" on page 172.

Table A-4 Process for imaging Mac computers (creating and deploying a Mac OS X automation image)

Step	Action	Description
Step 1	Install Mac OS X Server.	Install and configure the NetBoot server. See "About Installing Mac OS X Server software" on page 177.
Step 2	Create the preboot environment.	This step involves three primary steps, as follows: **1** Install Mac OS X on a computer. Ideally, the computer on which you install Mac OS X is not a production computer. This computer should be a lab Mac computer that you build and configure for the purpose of providing the source for creating preboot images. You can re-purpose this computer after you create the Mac OS X automation environment. The first two steps that are listed in this table are preparatory steps that you perform only once. **2** Install and configure the Deployment Solution agent (Darwin ADLagent). This step requires that you enable the automation role for the agent and then enable logging. **3** Create a NetBoot image. This step requires that you do three things. First, you create a disk image of the source computer. Then you import the disk image of the source computer into the Mac OS X NetBoot server using the System Imaging Utility. Finally, you enable the imported image for use as a NetBoot image. See "Creating a Mac OS X automation image" on page 178.

Table A-4 Process for imaging Mac computers (creating and deploying a Mac OS X automation image) *(continued)*

Step	Action	Description
Step 3	Perform imaging tasks.	Complete the following imaging tasks: **1** Capture images. **2** Deploy images. See "Performing imaging tasks" on page 190.

Performing management tasks

You perform Mac management tasks in the Deployment Solution Console.

See "Using Deployment Solution 6.9 to image Mac computers" on page 174.

This topic explains how to perform the Power Control tasks that are included with Deployment Solution 6.9. Details about how to create scripts are beyond the scope of this guide.

Power control lets you restart a managed Mac or shut it down.

You restart or shut down a computer by right-clicking a computer icon in the **Computers** pane and selecting **Power Control**. You complete the action by clicking **Operations > Power Control** on the menu bar or clicking the icon on the toolbar.

This task is a step in the process for managing Mac computers with Deployment Solution 6.9.

To perform Power Control management tasks

1 Right-click a computer and select **Power Control**.

A secondary menu displays the following options:

Wake-Up	Although this option appears in the secondary menu, it cannot be used with Mac clients.
Restart	Click to reboot the selected managed computer. Select **Force Applications to close without a message box** to restart immediately without prompting the user.
Shut down	Click to shut down the selected managed computer. Select **Force Applications to close without a message box** to shut down immediately without prompting the user.
Log off	Although this option appears in the secondary menu, it cannot be used with Mac clients.

2 Select a Power Control option.

3 In the **Confirm Operation** dialog box, select **Force application to close without a message** to shut down without giving users a warning.

If you do not select this option, the user is prompted to save work before the power operation continues.

4 Click **Yes**.

About Installing Mac OS X Server software

You must install and set up Mac OS X Server before you can create and deploy a Mac OS X automation image. This OS X automation image is a prerequisite to performing Mac imaging.

See "Using Deployment Solution 6.9 to image Mac computers" on page 174.

Installing Mac OS X Server is a step in the process for imaging Mac computers (creating and deploying a Mac OS X automation image).

See Table A-4 on page 175.

To set up Mac OS X Server properly for Deployment Solution 6.9 imaging, you must enable and configure the AppleTalk Filing Protocol (AFP), NetBoot, and Network File System (NFS) services. If you need help to install Mac OS X Server and to set it up properly, refer to Mac OS X Server Guides.

Creating a Mac OS X automation image

This topic guides you through creating the Mac OS X automation image. Creating and deploying a Mac OS X automation image is synonymous with creating a preboot environment.

For your reference throughout this part of the guide, note that Apple distinguishes between Mac OS X Server (the server software) and Mac OS X (the client software).

This procedure assumes that you have installed Deployment Solution 6.9 and a dedicated Mac server and that you have a separate Mac computer ready for creating the automation image.

If those assumptions are not true in your case, please complete the following tasks before you begin the process for creating and deploying a Mac OS X automation image:

- Install Deployment Solution 6.9 on a dedicated server or on the CMS server depending on your goals, as follows:

On a dedicated server	If you want to use the full functionality of Deployment Solution 6.9 to manage and image production Mac computers
On the same server where CMS 7.1 is installed	If you only want to image Mac computers using Deployment Solution 6.9 and have no plans to image Windows computers You can install on a dedicated server in this instance, but it is not necessary. Installing on the same server where CMS 7.1 is installed works too, as long as you have sufficient space.

- Set up a dedicated Mac server computer by installing Mac OS X Server software on supported hardware as specified by Apple.
  If you need help setting up Mac OS X Server, refer to Mac OS X Server Guides.
- Designate a second Mac computer solely for creating the Mac automation image. This task applies to everyone and prevents difficulties that you otherwise encounter. This task includes installing and configuring the Deployment Solution 6.9 agent.

Caution: The second Mac computer that you designate for creating the automation image must be the newest Mac hardware in your environment. If you create images on anything but the newest hardware in your environment, newer computers may not be able to boot from the images that you create.

Ideally, this second Mac computer is a lab Mac. You only need to dedicate this Mac temporarily. On this Mac you install Mac OS X software and then configure

and modify the source image. You then capture this image and use it as the automation image. The automation image is stored on the NetBoot (Mac OS X) server and runs from there. After you create the automation image and it is stored on the Mac OS X (NetBoot) server, you can repurpose the lab Mac. It is no longer needed for creating the Mac automation image.

The process that is outlined in this topic is a step in the process for imaging Mac computers (creating and deploying a Mac OS X automation image).

See Table A-4 on page 175.

Table A-5 Process for creating and deploying a Mac OS X automation image

Step	Action	Description
Step 1	Install Mac OS X on the source client.	This step requires that you complete the following tasks: ■ Install a new copy of Mac OS X on a system to be used as the source for your automation image. You may deselect all but the core installation files and Rosetta under the Custom settings for the installation. Rosetta is an option only in Mac OS X v10.6 (Snow Leopard). Refer to the Apple OS X installation guide for clients. ■ Run Software Update on the source computer and install any security or OS updates. See "Installing Mac OS X" on page 182.

Table A-5 Process for creating and deploying a Mac OS X automation image *(continued)*

Step	Action	Description
Step 2	Customize the source OS.	This step requires that you complete the following tasks: ■ Remove unnecessary files and applications from the source computer. A variety of third-party utilities are available that can assist with reducing the size of the source image. However, Symantec does not specifically endorse or provide support for the use of these utilities. The files to be removed can include OS language packs, input methods, and applications. ■ Modify the source computer's Energy Saver settings (**System Preferences > Energy Saver**) to disable system and hard disk sleep. ■ Rename the source computer (**System Preferences > Sharing**). Use a naming convention that makes it easy to identify a Mac OS X node that has been booted into automation. ■ Configure optional settings; for example, you can enable **Screen Sharing** and **Remote Login** on the **System Preferences	Sharing** menu. See "Customizing the source OS" on page 183.

Table A-5 Process for creating and deploying a Mac OS X automation image *(continued)*

Step	Action	Description
Step 3	Install the Darwin ADLagent.	This step requires that you complete the following tasks: ■ Copy the Darwin ADLagent installer from the Deployment Server (located in the **\Agents\ADLagent** folder of the **eXpress** share) to the source computer. ■ Install the Darwin ADLagent, providing the IP address of the Deployment Server and the Mac OS X (NetBoot) Server when prompted. A change was made in Mac OS X build 10.5.4 (Leopard). This change prevents the ADLagent installer from prompting the user for the IP addresses of the Deployment and Mac OS X (NetBoot) servers during installation. This problem was resolved in Mac OS X v10.6 (Snow Leopard). If you run any version of Mac OS X between 10.5.4 and 10.5.8, please refer to Symantec Knowledge Base article TECH41162 for more information. See "Installing the Darwin ADLagent" on page 184.
Step 4	Enable the Darwin ADLagent	The Darwin ADLagent runs on the Mac client computer. This step enables debug logging to assist with troubleshooting the imaging process. See "Enabling Darwin ADLagent logging" on page 185.
Step 5	Convert the Darwin ADLagent to the automation role.	This step causes the agent in the automation image to interact with the engine as an automation agent. See "Converting the Darwin ADLagent to an automation role" on page 186.

Table A-5 Process for creating and deploying a Mac OS X automation image *(continued)*

Step	Action	Description
Step 6	Add Share credentials to the source keychain.	Adding the Share credentials to the source keychain lets the agent access network file shares without user input. See "Adding Share credentials to the source keychain" on page 187.
Step 7	Capture the source image.	This step generates the base image that is used to create the NetBoot image. See "Capturing the source image" on page 187.
Step 8	Use the System Image Utility to convert the captured source image to a NetBoot image.	Apple provides a System Imaging document that provides the information that you need to create and manage images using the System Image Utility and NetBoot. However, you only use this utility after you have built a source computer using the procedures outlined in this appendix. Refer to the Apple System Imaging document. See "Creating the NetBoot image using the System Image Utility" on page 189.
Step 9	Configure NetBoot to use the newly created NetBoot image.	The NetBoot service does not run until it has a NetBoot image available for use. See "Setting up the NetBoot service" on page 189.

Installing Mac OS X

Perform this task on the system that you plan to use as the source for your automation image. You must retain the core installation files and Rosetta under the Custom settings for the installation. Note that Rosetta is an option only in Mac OS X 10.6 (Snow Leopard).

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To install Mac OS X

1 On the client Mac, install a new copy of Mac OS X.

For instructions from Apple, see the Snow Leopard Instructions.

2 Under the **Custom settings** for the installation, you can deselect all other files except for the core installation files and Rosetta.

3 On the Mac desktop, click the Apple icon in the upper left-hand corner of the screen, and on the drop-down menu select **Software Update**.

4 Install any security or OS updates.

Customizing the source OS

You customize the source OS by removing extraneous software from the system. However, the process for customizing the source OS on a Mac is completely different from working in Windows.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To customize the source OS

1 (Optional) Remove unnecessary files and applications from the source computer to reduce the size of the source image. Such files can include OS language packs, input methods, and applications.

Details about how to perform this step are beyond the scope of this document. It is optional in the process of creating an automation image.

This task is a typical task for Mac power users. A variety of third-party utilities can help you reduce the size of the source image. However, Symantec does not specifically endorse or provide support for the use of these utilities.

2 Modify the source computer's Energy Saver settings (**System Preferences > Energy Saver**) to disable system and hard disk sleep.

3 Rename the source computer (**System Preferences > Sharing**). Use a naming convention that makes it easy to identify a Mac OS X node that has been booted into automation.

4 Under **System Preferences > Sharing**, enable **Screen Sharing** and **Remote Login**.

This step enables extra diagnostic tools for the imaging process.

Installing the Darwin ADLagent

In this step you install and configure the agent to operate as an automation agent within the automation image.

This task is a step in the process for managing Mac computers with Deployment Solution 6.9.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To install the Darwin ADLagent

1. On the client Mac, on the Apple desktop, click the **Go** menu and select **Connect to Server**.
2. Copy the Darwin ADLagent installer from the Deployment Server to the source computer.

   In the **Connect to Server** window, enter the server address or hostname using the SMB protocol and a UNC path in the Server Address field. This protocol allows non-Windows systems to access Windows shares.

   The Darwin ADLagent installer is located in the **\Agents\ADLagent** folder of the **eXpress** share.

   Example: Enter `smb://Deployment/eXpress/` - and click **Connect**.
3. In the **\Agents\ADLagent** folder, copy the Darwin installation file to the source computer.
4. Install the Darwin ADLagent.
5. When you are prompted, provide the IP address of the Deployment Server and the Mac OS X Server (NetBoot).

Caution: A change was made in Mac OS X build 10.5.4 (Leopard). This change prevents the ADLagent installer from prompting the user for the IP addresses of the Deployment and Mac OS X (NetBoot) servers during installation. This problem was resolved in Mac OS X v10.6 (Snow Leopard). If you run any version of Mac OS X between 10.5.4 and 10.5.8, please refer to Symantec Knowledge Base article TECH41162 for more information.

Enabling Darwin ADLagent logging

In the event of a failure during imaging, the Darwin ADLagent captures information about the event. This information can assist Symantec support personnel in troubleshooting the cause of failure.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To enable client logging

1. On the client Mac, on the Apple desktop, click the **Finder** icon and select the system hard drive.
2. Then select the **Applications > Utilities** folder and double-click the **Terminal.app** file.
3. Edit the **/opt/altiris/deployment/adlagent/conf/adlagent.conf** file using the following command:

   ```
   sudo vi /opt/altiris/deployment/adlagent/conf/adlagent.conf
   ```

   Using the sudo command prompts the user to enter an administrator password.
4. Press the **I** key to enable Insert mode.
5. Change the value **Debug_Trace=false**' to '**Debug_Trace=true**.
6. Change the value **IPTrace=false** to **IPTrace=true**.
7. Change the value **IPUseLogFile=false** to **IPUseLogFile=true.**
8. For additional debug-level logging, add the following entry at the end of the file:

   ```
   DEBUG_LOG=true
   ```
9. Press **Esc**.
10. Press the **:** key, and then press **wq!**.
11. Press **return**.
12. Edit the **/opt/Altiris/deployment/adlagent/conf/trace.conf** file using the following command:

    ```
    sudo vi /opt/altiris/deployment/adlagent/conf/trace.conf
    ```
13. Press the **I** key to enable Insert mode.
14. Change the value **#TcpTracePort=415** to **TcpTracePort=415**

15 Change the value **#TcpTraceIP=192.168.1.1** to **TcpTraceIP=IP address of the Deployment Server**

16 Press **Esc**.

17 Press the **:** key, and then press **wq!**.

18 Press **return**.

Converting the Darwin ADLagent to an automation role

(For imaging only)

You perform this task on the source Mac using the Mac OS X Terminal (Terminal.app). Assuming that you opened the Terminal to enable the Darwin ADLagent and have just completed that task, the Terminal should still be open.

If you have closed the Terminal, open it again: On the source Mac, in the Dock, click the **Finder** icon and select the system hard drive. Then select the **Applications > Utilities** folder and double-click the **Terminal.app** file.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To convert the Darwin ADLagent to an automation role

1 Edit the **/etc/altiris/deployment/agent-install.conf** file using the following command:

```
sudo vi /etc/altiris/deployment/agent-install.conf
```

2 Press the **I** key to enable Insert mode.

3 Change the value **export OS_TOOLBOX=darwin** to **export OS_TOOLBOX=automation**.

4 Press **Esc**.

5 Press the **:** key, and then press **wq!**.

6 Press **return**.

7 Run the installation for the Darwin ADLagent again.

Adding Share credentials to the source keychain

You add Share credentials to the source keychain to ensure that no user interaction is required during imaging. The credentials to network file shares are stored within the automation image. These credentials are made accessible to the automation agent through the system Keychain application.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To add Share credentials to the source keychain

1. On the **eXpress** share in the **\TechSup\Macintosh** folder on the Deployment Server copy the **AddCredentialsToKeychain** utility to the source computer.
2. If you changed the logging path when you converted the Darwin ADLagent to an automation role, you must enter credentials to the Deployment Server. Otherwise, logs are not saved in the eXpress share.

   To enter credentials, extract and run **AddCredentialsToKeychain.app** and provide all the requested information.

   Note that an AppleTalk Filing Protocol (AFP) share must be used for the storage of image files. Neither the eXpress share nor its subfolders is a valid target for Mac image files.
3. At the prompts click **Allow** or **Allow All**.

Capturing the source image

After you configure the source OS, you must capture it as a disk image. This step prepares the OS to be converted to a NetBoot image.

You perform this task in the Terminal on the Mac client. The Mac client is the source of the image that you need to capture.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To capture the source image

1. On the source computer, click **Finder > Go > Connect to Server > SMB://*OS X server name*/NetBootClients0** to connect to the Mac OS X (NetBoot) server's **NetBootClients0** share.
2. Open the Terminal and enter the following command:

   ```
   sudo hdiutil create -srcfolder /Volumes/source_disk
   /Volumes/NetBootClients0/SystemRO.dmg.
   ```

   You must insert a space between `/Volumes/source_disk` and `/Volumes/NetBoot Clients0/SystemRO.dmg`.

   You must also use the backslash (\) escape character in place of a space in the hard drive name. For example, if the hard drive name is Macintosh HD, you enter the src command as follows:

   ```
   -srcfolder /Volumes/Macintosh\ HD/
   ```

   Replace *source_disk* with the name of the source computer's primary drive.
3. In the Terminal, enter the following command to convert the read-only image to read-write:

   ```
   hdiutil convert /Volumes/NetBootClients0/SystemRO.dmg –format
   UDRW –o /Volumes/NetBootClients0/System.dmg
   ```
4. In the Terminal, determine the image size by entering the following command:

   ```
   ls -lh /Volumes/NetBootClients0/System.dmg
   ```

   Locating the image size helps you determine what to change in the following step.
5. In the Terminal, enter the following command to add another 1 GB of padding to the image:

   ```
   hdiutil resize -size newsize /Volumes/NetBootClients0/System.dmg
   ```

   Replace **newsize** with the desired size; for example, for a 3 GB image plus 1 GB padding, enter the following command:

   ```
   hdiutil resize -size 4g …
   ```
6. In the Terminal, delete the **SystemRO.dmg** file by entering the following command:

   ```
   sudo rm /Volumes/NetBootClientsSPO/SystemRO.dmg
   ```

Creating the NetBoot image using the System Image Utility

After you capture a disk image of the source OS, you must convert the image for use as a NetBoot image.

You use the System Image Utility that is included with Mac OS X Server to perform this conversion.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To create the NetBoot image

1. On the NetBoot server, navigate to **/Library/NetBoot/NetBootClients0** and open the **System.dmg** file.
2. Open the System Image Utility **/Applications/Server/System Image Utility.app**.
3. Select **NetBoot Image** for the Network Disk image to be created.
4. Click **Continue**.
5. Enter a name and corresponding details for the NetBoot image, and click **Create**.
6. Exit the System Image Utility.

Setting up the NetBoot service

After you create the NetBoot image, you must enable the NetBoot image on the Mac OS X Server computer. The NetBoot service on Mac OS X Server cannot run until you have enabled a valid NetBoot image.

The steps that are presented in this topic are sufficient to let you image Mac computers. If you need or want more advanced configuration information, refer to the System Imaging and Software Update Administrator Guide from Apple Corporation for the version of OS X that you are using.

This task is a step in the process of creating and deploying a Mac OS X automation image.

See "Creating a Mac OS X automation image" on page 178.

To set up the NetBoot service

1. On the Mac OS X Server computer, open the Server Admin utility (**/Applications/Server/Server Admin.app**) and connect to Mac OS X Server.
2. Click the triangle to the left of the server.
3. In the expanded **Servers** list, click **NetBoot**.
4. Click **Settings**, and then click **Images**.
5. Enable the images that you want your clients to use, enable the diskless option, and choose the Network File System (NFS) protocol.
6. In the **Default** column, check the box to set the default image.
7. Click **Save**.

   At this point, the preboot environment is set up.

Performing imaging tasks

Imaging tasks include creating a Mac image and deploying a Mac image.

See Table A-4 on page 175.

You use the **Create Disk Image** task to create a Mac image.

See "Creating a Mac image" on page 190.

After you create a Mac image, you deploy it by distributing the Mac image file to managed computers.

See "Deploying a Mac image" on page 191.

Creating a Mac image

1. On the Deployment Server, in the Deployment Solution 6.9 Win32 console, in the **Create Disk Image** dialog box, from the **Imaging Tool** drop-down list, select **Mac Image (*.dmg)**.
2. In the **Additional Parameters** field, enter the disk number using the following format:

   ```
   -d[disk#]
   ```

   To image a different disk, in the **Additional Parameters** enter the disk number field using the same format.
3. Choose from one of the following options to add the path name and file name for the disk image:

   - Specify the share using the following format:

     ```
     afp://server/sharepoint/path/filename.dmg
     ```

- Provide credentials using the following format:
  `afp://username:password@server/sharepoint/path/filename.dmg`

If no credentials for this server are provided in the automation configuration, the guest account is used by default.

Warning: These credentials are passed unencrypted, and a network sniffer can read them.

Caution: The captured disk image must be stored on an AppleTalk Filing Protocol (AFP) share.

---

4 Select **Disable image path validation**.

The image file is stored outside of the Deployment Share file structure. If you do not select this option, a warning message appears. This message reminds you to configure your automation process to use the path that is indicated in the **Name** field. You can still save your image to a location outside of the Deployment Share file structure even when you do not select this option. This option eliminates the warning message.

5 Select the **Do not boot to Production** option if you do not want the computer to boot to Production before you create the image.

6 In the **Automation pre-boot environment (DOS/WinPE/Linux)** drop-down list, select **Default Automation (Auto-select)**.

7 Click **Next**.

8 (Optional) In the **Return Codes** dialog box, set Return Codes.

9 Click **Finish**.

The task appears in the **Task** list for the job. The Mac image is created when you run this task.

Deploying a Mac image

1 On the Deployment Server, in the Deployment Solution 6.9 Win32 console, in the **Distribute Disk Image** task, select **Select a disk image file**.

2 In the **Name** field, choose from one of the following options to add the path to the Mac (.DMG) image:

- Specify the share using the following format:
  `afp://server/sharepoint/path/filename.dmg`

- If you did not run the **AddCredentialToKeychain** application when you created the automation image, provide credentials using the following format:

  ```
  afp://username:password@server/sharepoint/path/filename.dmg
  ```

If no credentials for this server are provided in the automation configuration, the guest account is used by default.

Warning: These credentials are passed unencrypted, and a network sniffer can read it.

Caution: The captured disk image must be stored on an AppleTalk Filing Protocol (AFP) share.

---

3. Select **Automatically perform configuration task after completing this imaging task** to run the configuration task after the imaging task is complete.
4. Click **Next**.
5. (Optional) In the **Return Codes** dialog box, set Return Codes.
6. Click **Finish**.

   The task appears in the **Task** list for the job. The Mac image is deployed when you run this task.

   The **Image is stored locally on the client** and the **Sysprep settings** options are disabled when you select a Mac image. The **Select a computer on the network**feature is not supported when you use Mac Imaging. The **Automation pre-boot Environment** for Mac Image is **Default Automation** when you deploy Mac images. This option uses the NetBoot architecture that was previously set up.

Appendix B

Troubleshooting

This appendix includes the following topics:

- About Symantec Notification Manager
- Installing the Symantec Management Agent for Mac
- Launching the Symantec Management Agent for Mac GUI
- Using the Symantec Management Agent for Mac GUI

About Symantec Notification Manager

Symantec Notification Manager is an application that displays administrative alerts before it runs a task or restarts the computer. Symantec Notification Manager is a part of the Symantec Management Agent for Mac. ()

For example, the Notification Server computer administrator can create a software installation task that requires the computer to be restarted. Before it restarts the computer, Symantec Notification Manager displays an alert. The alert asks the currently logged-in user to close all programs.

If you miss an alert, you can open Symantec Notification Manager. To open the manager, click **Active Alerts** in the Symantec Management Agent for Mac GUI and view the list of active alerts for all users. (See "Using the Symantec Management Agent for Mac GUI" on page 194.)

Installing the Symantec Management Agent for Mac

The Notification Server computer administrator installs the Symantec Management Agent for Mac. To install the Symantec Management Agent for Mac refer to your Notification Server documentation.

Launching the Symantec Management Agent for Mac GUI

You can launch the Symantec Management Agent for Mac graphical user interface (GUI) on the Macintosh computer. Navigate to /Applications/Utilities/ and open the Symantec Management Agent application.

You can drag the Symantec Management Agent icon into the Dock for convenient access.

Using the Symantec Management Agent for Mac GUI

The Symantec Management Agent for Mac graphical user interface (GUI) contains the following sections:

- Agent Details
- Special Periods
- Software Management
- Task Management

Each GUI section includes several options.

Table B-1 Options in the Agent Details section

Option	Description
General	The General group displays the following Symantec Management Agent information: ■ The Notification Server computer address with which the Symantec Management Agent for Mac is registered. ■ The version of Notification Server software. ■ The unique identifier of the Macintosh computer. This identifier is used to register the computer with Notification Server. The Client Configuration group displays the following information: ■ The last time the Symantec Management Agent for Mac requested a client configuration file from Notification Server. ■ The last time an updated client configuration file was received. ■ How often the Symantec Management Agent for Mac should query Notification Server for a new client configuration file. The client configuration policy defines this parameter. (For more information, see the *Notification Server User Guide*.) To request the client configuration manually, click **Refresh Now**. The **Basic Inventory** group displays the following information: ■ The last time that the Symantec Management Agent sent the computer identification information to Notification Server. Computer information includes hardware and software inventory. ■ Basic inventory send interval, as defined by the client configuration policy. (For more information, see the *Notification Server User Guide*.) To send basic inventory manually, click **Send Now**.

Table B-1 Options in the Agent Details section *(continued)*

Option	Description
Plug-ins	Displays the Symantec Management Agent for Mac plug-ins that are registered on the managed Macintosh computer. Displays the plug-in version and installation directory.
Policies	Displays the client configuration policies that apply to the managed Macintosh computer, as defined by the Notification Server computer administrator. To request configuration policies from the server, click **Refresh Configuration Now**. To view details of the configuration policy, click **Show Details**.
Active alerts	Click to launch the Symantec Notification Manager application. This application displays the active alerts that precede administrative task execution and computer restarts. See "About Symantec Notification Manager" on page 193.
Log Viewer	Click to launch the console application and view the Symantec Management Agent for Mac log. The default log level is **error**. For information about changing the log level, see the *Notification Server User Guide*.

Table B-2 Options in the Special Periods section

Option	Description
Maintenance windows	Displays the maintenance windows, as defined by the Notification Server computer administrator. When maintenance windows are defined, tasks can be run only within the specific periods of time. For more information, see the *Notification Server User Guide*.

Table B-2 Options in the Special Periods section *(continued)*

Option	Description
Network blockouts	Displays the network communication blockouts, as defined by the Notification Server computer administrator. When a network communication blockout is active, network traffic between the Symantec Management Agent and Notification Server is reduced. For more information, see the *Notification Server User Guide*.
Bandwidth throttling	Displays the network bandwidth throttling settings, as defined by the Notification Server computer administrator. When bandwidth throttling is enabled, the bandwidth that the Symantec Management Agent for Mac uses is limited. For more information, see the *Notification Server User Guide*.

Table B-3 Option in the Software Management section

Option	Description
Software Delivery	Displays the Software Management Solution tasks that are available for the managed Macintosh computer. To check if any new tasks are available for this computer, click **Refresh Tasks from Server**. To view details of available tasks, or to run or suspend a task, click **Show Details**. For more information, see the Software Management Solution user guide .

Table B-4 Options in the Task Management section

Option	Description
Client Task Agent	The Connectivity group shows the task server with which the Client Task Agent is registered. It also shows the connection status of the Client Task Agent. To force registration with the task server, click **Register**. The Client Tasks group shows the number of active tasks that are assigned to this managed Macintosh computer by the task server. To check if any new tasks are available for this computer, click **Check for New Tasks**. For more information, see the Task Server user guide .
Client Tasks	Displays the list of tasks that are assigned to this managed Macintosh computer by the task server. To manually check if any new tasks are available, click **Check for New Tasks**. To view finished tasks, click **Show Tasks History**.

Index

A

about configuration
  Symantec Management Agent for Mac computers 55
Access Server
  settings for remote management with pcAnywhere 162
advanced options
  Managed Software Delivery 117
  Software Management Solution tasks 118
advanced software delivery. *See* Managed Software Delivery
agent 110–111
  See also plug-in
  See also plug-ins
agent connectivity credentials
  global Symantec Management Agent settings 60
agent settings for Mac computers
  Agent Settings tab
    Installation Settings dialog box 51
Altiris Agent. *See* Symantec Management Agent
applicability check
  about 126

B

blockout period
  adding to targeted agent settings policy 71
  settings 70

C

checking agent installation
  Mac installation prerequisites 34
command-line options
  managing Mac client computers 35
compliance
  checking 151
compliance check
  about 126
  how it works 125
  schedule settings 113
components
  Software Management Solution 107
computer
  pulling Symantec Management Agent for UNIX, Linux, and Mac 43
  pushing Symantec Management Agent for UNIX, Linux, and Mac 41
configuration
  Symantec Management Agent for Mac computers 56
configuration settings
  Symantec Management Agent for Mac 65
Connection and Authentication tab
  Installation Settings dialog box 46
creating a Mac OS X automation image 178
CSV file
  importing Mac computers 36, 38

D

Darwin ADLagent
  converting to an automation role 186
  enabling logging 185
  installing 184
deploying Symantec Management Agent to Mac OS X client computer
  Mac installation prerequisites 33
Deployment Solution 6.9
  setting up Mac OS X Server for imaging 177
  using to image Mac computers 174
  using to manage and image Mac computers 172
  using to manage Mac computers 172
  using to perform Mac management tasks 176
destination download location
  setting 115
digitally signed packages
  Mac firewall
    about 53
disabling or configuring built-in Mac OS X firewall
  Mac installation prerequisites 28
discovering Mac computers 77
  Network Discovery wizard 79

discovering Mac computers *(continued)*
with manually created tasks 80
discovery Mac computers
about 77
DMG file
creating to deliver software to Mac OS X computers 136
download location, package
alternate 115
default 115
Symantec Management Agent cache 115
download settings
Software Management Solution 114

E

encryption
settings for remote control with Mac computers 161

F

filescan.rule file
using to scan for files on Mac computers 96

H

home page 157
hosting an internal SUS
about 144

I

implementation
Software Management Solution 109
implementing
Patch Management Solution for Mac 150
incoming connections to Mac computers
through Secure Shell (SSH) 32
installation prerequisites for Mac agent and plug-ins 21
checking agent installation 34
deploying Symantec Management Agent to Mac OS X client computer 33
disabling or configuring built-in Mac OS X firewall 28
setting up Notification Server name resolution 27
installation settings
Symantec Management Agent for UNIX, Linux, and Mac 44
Installation Settings dialog box 45
Agent Settings tab for Mac computers 51
Connection and Authentication tab 46
login and password settings 48
platform detection settings 51
SSH authorization settings 47
SSH password authorization settings 48
timeout settings 50
Install XML tab for Mac computers 52
installer
importing into the Software Catalog
to deliver software to Mac OS X computers 138
Installer Shell script
creating
to deliver software to Mac OS X computers 137
installing Mac agent and plug-ins 24
about 20
installing Mac computers with pull (manual) agent installation 43
about 42
installing Mac computers with push (automatic) agent installation
about 39
internal Software Update Server (SUS)
about hosting to obtain internal software updates 144
inventory information
about Mac computers
gathering, using a policy 88
gathering, using a task 90
custom, about Mac computers
gathering, using a task 91–92
inventory reports
viewing for Mac computers 97
Inventory Solution
information gathered with a policy
checking 101
information gathered with a task
checking 102
troubleshooting Mac problems 98, 102
using on Mac computers 84
Inventory Solution for Mac
about 87
Inventory Solution plug-in
checking deployment on Mac computers 100
deploying to the Mac OS X computer 86

Inventory Solution policy
troubleshooting Mac problems 99
inventory tasks and data
for Mac computers 85
inventorying computers 151

K

key CMS Mac capabilities and limitations
compared to Windows 13

L

local Software Update Server (SUS)
redirecting a Mac client computer 145
login and password settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 48
login settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 48

M

Mac agent and plug-ins
about 35
installation prerequisites 21
installing 20, 24
Mac client computer
redirecting to a local Software Update Server (SUS) 145
Mac client computers
about selecting for Symantec Management Agent pull (manual) installation 36
creating .csv file for computer details 38
managing with command-line options 35
selecting for Symantec Management Agent pull (manual) installation 37
Mac computers 106
See also UNIX, Linux, and Mac
about discovering 77
about gathering custom inventory information 91
about imaging 168
about Inventory Solution 87
about limitations of imaging 171
about managing with CMS 9
key CMS capabilities and limitations 13
supported package-delivery formats 14
about software inventory using the filescan.rule file 94
Mac computers *(continued)*
about supported package-delivery formats 14
about using Deployment Solution 6.9 to manage and image 172
Access Server settings 162
agent connectivity credentials 60
and pcAnywhere 159
and remote control 159, 163
and remote control communication requirements 161
blockout period settings 70
checking deployment of the Inventory Solution plug-in 100
checking the inventory information that is gathered with a policy 101
checking the inventory information that is gathered with a task 102
configuring blockout periods 71
configuring maintenance window 74
configuring software delivery tasks 134
configuring Symantec Management Agent policies 55–56
deploying the Inventory Solution plug-in 86
discovering 77
discovering with tasks created manually 80
discovering with tasks using the wizard 79
download throttling settings 67
enabling devnote logging for troubleshooting 99
enabling power management in targeted settings policy 72
ensuring that they can receive the Inventory Solution policy 99
gathering custom inventory information 92
gathering inventory information 88, 90
general targeted agent settings 64
global agent settings 56–57
installing the Inventory Solution plug-in 102
key CMS capabilities and limitations 13
maintenance window 73
multicast settings 67
Notification Server Event Capture settings 60
package multicast settings 60
power management settings 58
remote control authentication settings 162
remote control connection settings 161
sample task, creating a DMG file to deliver software 136

Mac computers *(continued)*
sample task, creating a Managed Software Delivery policy to deliver software to Mac OS X computers 140
sample task, creating a task to disable the Product Improvement pop-up 140
sample task, creating an Installer Shell script to deliver software 137
sample task, importing an installer into the Software Catalog to deliver software 138
scanning using the filescan.rule file 96
setting alternate NS URL 72
software inventory using the filescan.rule file 96
support in Software Management Solution 106
Symantec Management Agent data update intervals 64
system requirements for imaging 169
targeted agent settings 61
targeted Mac agent settings 65
tickle settings 58
troubleshooting problems using devnote logging 99
troubleshooting problems with Inventory Solution 98
types of inventory tasks and data 85
user control settings 72
using Deployment Solution 6.9 to image 174
using Deployment Solution 6.9 to manage 172, 176
using Inventory Solution 84
using tasks to manage 133
viewing inventory data in Resource Manager 97
viewing inventory reports 97
Mac firewall
digitally signed packages
about 53
Mac image
creating 190
creating and deploying 190
deploying 190
Mac imaging
about installing Mac OS X Server 177
about limitations 171
about using Deployment Solution 6.9 172
process for creating Mac OS X automation image 178
Adding Share credentials to the source keychain 187
Capturing the source image 187
Mac imaging *(continued)*
process for creating Mac OS X automation image *(continued)*
Converting the Darwin ADLagent to an automation role 186
Creating the NetBoot image using the System Image Utility 189
customizing the source OS 183
Enabling Darwin ADLagent logging 185
installing Mac OS X 182
installing the Darwin ADLagent 184
Setting up the NetBoot service 189
system requirements 169
using Deployment Solution 6.9 174
Mac imaging environment
about setting up 168
Mac imaging tasks
creating a Mac image 190
deploying a Mac image 190
performing 190
Mac management
using Deployment Solution 6.9 172
Mac management tasks
performing with Deployment Solution 6.9 176
Mac OS X
creating automation image 178
imaging 190
installing 182–187, 189
Mac OS X automation image
creating 178
Mac OS X client computer
checking agent installation 34
deploying Symantec Management Agent 33
Mac OS X firewall
disabling or configuring 28
Mac OS X Server
about installing 177
Mac software
how patching works 144
Mac Terminal 20, 32
See also Secure Shell (SSH)
maintenance window
about 73
configuring policy 74
Managed Software Delivery
about 121
actions 122
advanced options 117
compliance. *See* compliance check

Managed Software Delivery *(continued)*
execution process 123
key tasks 122
policy creation 127
Policy Rules/Actions. *See* settings, Managed Software Delivery
remediation. *See* remediation, software
settings. *See* settings, Managed Software Delivery
software resource, selecting 130
task
adding 130
settings 131
wizard 127
managing Mac computers with CMS
about 9
multicast
global Symantec Management Agent settings 60

N

NetBoot image
creating 189
NetBoot service
setting up 189
Network Discovery 79–80
process 77, 79
task 80
wizard 78
Network Discovery task
creating 79–80
location 79–80
modifying 80
Network Discovery wizard 79–80
Notification Server Event Capture settings
global Symantec Management Agent settings 60
Notification Server name resolution
Mac installation prerequisites 27

O

options, Managed Software Delivery. *See* settings, Managed Software Delivery
options, Software Management Solution. *See* settings, Software Management Solution

P

Package Delivery
advanced options 118
package download
alternate location 115
default location 115
Managed Software Delivery 125
Symantec Management Agent cache 115
package multicast settings
global Symantec Management Agent settings 60
password authorization settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 48
password settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 48
Patch Management Solution for Mac
about 149
implementing 150
return codes 155
patching Mac software
about 143
See also Patch Management Solution for Mac
how it works 144
See also Patch Management Solution for Mac
pcAnywhere
authentication settings with Mac computers 162
communication requirements with Mac computers 161
connection settings with Mac computers 161
installing the plug-in 163
with Mac computers 159, 162
pcAnywhere plug-in
installing 163
platform detection settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 51
platform support, Software Management Solution 106
plug-in 110–111
See also agent
See also Software Management Solution plug-in
policy
data update intervals 64
gathering inventory information about Mac computers 88
general targeted agent settings 64
global agent settings 56–58
global authentication settings 60
global event settings 60

policy *(continued)*
maintenance window policy 74
package multicast settings 60
targeted agent settings 61
Policy Rules/Actions. *See* settings, Managed Software Delivery
policy to deliver software to Mac OS X computers
creating 140
portal
Software Portal. *See* Software Portal
portal page 157
prerequisites
Symantec Management Agent for Mac installation 21
process for creating Mac OS X automation image 178
Adding Share credentials to the source keychain 187
Capturing the source image 187
Converting the Darwin ADLagent to an automation role 186
Creating the NetBoot image using the System Image Utility 189
customizing the source OS 183
Enabling Darwin ADLagent logging 185
installing Mac OS X 182
installing the Darwin ADLagent 184
Setting up the NetBoot service 189

Q

Quick Delivery
advanced options 118

R

recurring software delivery
scheduling 113
remediation, software
about 126
how it works 126
schedule settings 114
remote control
Access Server settings with Mac computers 162
authentication settings with Mac computers 162
communication requirements with Mac computers 161
connection settings with Mac computers 161
encryption settings with Mac computers 161
installing the pcAnywhere plug-in 163
plug-in 163
remote control *(continued)*
with Mac computers 159
remote management
with Access Server 162
reports 155
viewing 156
Resource Manager
viewing inventory data of Mac computers 97
results-based actions
Software Management Solution 116
return codes
patch management for Mac 155
run settings
Software Management Solution 115

S

schedule settings
compliance check 113
Managed Software Delivery 112
remediation 114
Secure Shell (SSH) 20, 32
See also Mac Terminal
authorization settings 47
password authorization settings 48
security
Software Management Solution 110
Select Software dialog box 128
select software resource
Managed Software Delivery 130
selecting Mac computers for pull (manual) agent installation 37
about 36
settings, Managed Software Delivery
advanced options 117
compliance 113
download 114
Policy Rules/Actions 129
policy settings 131
remediation 114
run 115
schedule 112
software 129
settings, Software Management Solution
default 111
download 114
results-based actions 116
task. *See* task options, Software Management Solution

software delivery 121
See also Managed Software Delivery
advanced 121–122
methods 119
software delivery tasks for Mac computers
configuring 134
software inventory
and filescan.rule file on Mac computers 96
about 94
Software Management Solution 111, 132
See also settings, Software Management Solution
See also Software Portal
components 107
delivering Mac software 106
implementing 109
key tasks 108
settings. *See* settings, Software Management Solution
Software Management Solution agent. *See* Software Management Solution plug-in
Software Management Solution plug-in
Mac
about 111
Software Portal 132
See also software request
about 132
Software Update Server (SUS)
about hosting 144
redirecting a Mac client computer 145
software updates
installing all updates 154
installing individual updates 152
obtaining by hosting an internal SUS 144
viewing available 152
viewing installation status 156
solution plug-ins for Mac computers
about 35
source image
capturing as a disk image 187
source keychain
adding Share credentials 187
source path update
advanced options 118
specifying agent installation settings
Symantec Management Agent for Mac computers 44
SSH Key authorization settings
Connection and Authentication tab
Installation Settings dialog box 47
supported package-delivery formats
for Mac software distribution in CMS 14
SUS. *See* Software Update Server
Symantec Management Agent
about installing on Mac computers with a pull (manually) 42
configuring agent policies for Mac 55
data update intervals 64
importing Mac computers from .csv file 36, 38
installing on Mac computers with a push (automatically) 39
selecting Mac computers for installation 36–37
Symantec Management Agent cache 115
Symantec Management Agent for Mac
about configuring for Mac computers 55
about general settings for Mac 58, 60
about package multicast settings for Mac computers 60
about power management settings for Mac computers 58
about tickle settings for Mac computers 58
agent connectivity credentials 60
blockout period settings 70
configuration settings 65
configuring agent policies for Mac 56
configuring blockout periods 71
configuring for Mac computers 56
configuring general settings for Mac 57
configuring maintenance window policy 74
configuring power management settings for Mac computers 57
configuring tickle settings for Mac computers 57
download throttling settings 67
enabling power management in targeted settings policy 72
general targeted settings 64
global settings 56–58
installation settings
Install Settings dialog box 45
local settings 61
maintenance window 73
multicast settings 67
Notification Server Event Capture settings 60
selecting computers for installation 37
setting alternate NS URL 72
specifying installation settings 44
targeted settings 61
user control settings 72

Symantec Management Agent for Mac 7.1
about Symantec Notification Manager 193
installing 193
launching the GUI 194
using the GUI 194
Symantec Management Agent for UNIX, Linux, and Mac
installation settings
specifying 44
push installation process 39
Symantec Management Agent for UNIX, Linux, or Mac
.csv template file 38
about installing with a pull (manually) 42
importing computers from .csv file 36, 38
installation requirements 21
installation settings 45
agent execution settings 51
agent settings 51
agent settings, preserving 51
authentication settings 46
command timeout setting 50
configuration 52
connection settings 46
login and password 48
login settings 48
login timeout setting 50
package upload speed setting 50
password settings 48
platform detection settings 51
privileged user account settings 48
SSH password authorization settings 48
startup 52
unprivileged user account settings 48
upgrade 52
upgrade, configuration, and startup 52
XML format for manual installation 52
installation settings, Agent Settings tab 51
installation settings, Connection and Authentication tab 46
login and password settings 48
platform detection settings 51
SSH key authorization settings 47
SSH password authorization settings 48
timeout settings 50
installation settings, Install XML tab 52
installing on Mac computers 20, 24
installing on selected computers 41
installing with a pull (manually) 43
Symantec Management Agent for UNIX, Linux, or Mac *(continued)*
installing with a push (automatically) 39
Mac installation prerequisites 21
prerequisites 21
pulling from the console to Mac computers 43
pushing to computers 41
selecting computers for installation 36
simultaneous installation tasks, setting 41
Symantec Notification Manager
about 193

T

task
gathering inventory information about Mac computers 90
task options, Software Management Solution
about 112
defaults, overriding 118
task settings, Software Management Solution. *See* task options, Software Management Solution
task to disable the Product Improvement pop-up
creating 140
task, Software Management Solution
advanced options 118
options. *See* task options, Software Management Solution
settings, default 111
tasks
using to manage Mac computers 133
timeout settings for Mac computers
Connection and Authentication tab
Installation Settings dialog box 50
troubleshooting
Mac problems with Inventory Solution 98–102

U

UNIX, Linux, and Mac
support in Software Management Solution 106
updates. *See* software updates
updating computers
checking needed updates 151
installing all updates 154
installing individual updates 152
viewing available updates 152
viewing status reports 156
updating Mac software. *See* patching Mac software

upgrade, configuration, and startup settings for Mac computers
Install XML tab for Mac computers
Installation Settings dialog box 52

W

Windows Installer repair
advanced options 118